BAN-GZKP: Optimal Zero Knowledge Proof based Scheme for Wireless Body Area Networks

Gewu Bu, Maria Potop-Butucaru

BAN-GZKP: Optimal Zero Knowledge Proof based Scheme for Wireless Body Area Networks[☆]

Gewu Bu[a], Maria Potop-Butucaru[a]

[a]*Sorbonne Université, UPMC, LIP6, CNRS UMR 7606*

Abstract

BANZKP is the best to date Zero Knowledge Proof (ZKP) based secure lightweight and energy efficient authentication scheme designed for Wireless Area Network (WBAN). It is vulnerable to several security attacks such as the replay attack, Distributed Denial-of-Service (DDoS) attacks at sink and redundancy information crack. However, BANZKP needs an end-to-end authentication which is not compliant with the human body postural mobility. We propose a new scheme BAN-GZKP. Our scheme improves both the security and postural mobility resilience of BANZKP. Moreover, BAN-GZKP uses only a three-phase authentication which is optimal in the class of ZKP protocols. To fix the security vulnerabilities of BANZKP, BAN-GZKP uses a novel random key allocation and a Hop-by-Hop authentication definition. We further prove the reliability of our scheme to various attacks including those to which BANZKP is vulnerable. Furthermore, via extensive simulations we prove that our scheme, BAN-GZKP, outperforms BANZKP in terms of reliability to human body postural mobility for various network parameters (end-to-end delay, number of packets exchanged in the network, number of transmissions). We compared both schemes using representative convergecast strategies with various transmission rates and human postural mobility. Finally, it is important to mention that BAN-GZKP has no additional cost compared to BANZKP in terms memory, computational complexity or energy consumption.

Keywords: Wireless Body Area Network (WBAN), Mobile and wireless security, Network performance analysis, Zero Knowledge Proof (ZKP)

1. Introduction

Wireless Body Area Networks (WBAN) is a special kind of Wireless Sensors Networks (WSN). In WBAN, networked body sensors collect user's physiological data and transmit them to a sink node. There is a tremendous difference between WBAN and classical WSN. In WBAN nodes are distributed on/in human body and, similar to the Delay-Tolerance Networks (DTN), move with the human postural mobility [1], [2]. Because of that, the network topology in Intra-WBAN dynamically changes following the postural body mobility. In a recent work related to channel modes for WBAN [3] the authors advocate for the use of multi-hops communication in WBAN.

Multi-hop WBAN communication schemes easily adapt to postural mobility where nodes and links are highly dynamic [3]. Also, multi-hop communications need lower transmission power compared to one-hop direct communication where source nodes have to use enough transmission power in order to make sure that their messages can reach the sink directly. Moreover, lower transmission powers automatically reduce the radio radiation of the human body, which became an important issue today [3].

However, multi-hop communication in WBAN is vulnerable to security and privacy attacks. Any medical data error, leakage or imitation may lead to a wrong medical treatment. The disclosure of critical health information can also have irreversible consequences on the patients daily life. Security mechanisms are thus needed in WBAN to protect user's data from malicious eavesdropping, tampering or abuse.

[☆]An extended abstract of this paper appeared in IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017

Email addresses: gewu.bu@lip6.fr (Gewu Bu), maria.potop-butucaru@lip6.fr (Maria Potop-Butucaru)

Recently, the literature investigated Inter-WBANs security. As examples, [4], [5] and [6] discuss the security mechanism for communications from the sink to the remote Health Centre (hospitals or online doctors). In this context the security of the Intra-WBAN communication should also be carefully considered: date leakage or tampering of source nodes from Intra-WBAN area leads to a meaningless subsequent Inter-WBAN security protection.

The challenges of Intra-WBAN security are threefold:

- The computing capacity of WBAN devices is limited. Traditional encryption and decryption algorithms used for personal computers or mobile phones may be not applicable as they are to the WBAN devices.
- Poor storage of WBAN devices may not be able to store too much shared content to make effective the recent complex authentication and security protocols.
- Control message exchanges may lead to poor applicative performances.

Related Works. The most basic encryption mechanism, symmetric encryption, uses the same secret key to encrypt and decrypt data. As symmetric key can be directly used in Stream cipher or Block cipher, the coding speed and its efficiency are very competitive. However, in symmetric encryption, by using the all-networks-widely fixed key, if one node has been compromised, the secret key will be known by adversary who can then monitor the entire networks. Also, symmetric encryption suffers from replay attack due to the use of the same encryption key. Some improvement solutions come out to solve the replay attack problem. One example is MiniSec [7]. Without using the same key, MiniSec uses data sequence as a part of encryption key. However, MiniSec needs to synchronize sequences of packets when the number of missing messages is important. This is often the case in a WBAN environment. Also MiniSec suffers from DDoS attack at the sink, since MiniSec doesn't force a hop-by-hop authentication, malicious message traffic from adversary can deliver to all the network. Other solutions [8], [9] and [10] come with specified *Key Agreement Mechanism* to ensure the key will change periodically. However, most of works do not mention the networks performance impact when applied in a real WBAN environment.

Public Key Infrastructure (PKI) is a widely-used asymmetric encryption, authentication and access control mechanism ([11], [12]). Especially after the introduction of elliptic curve encryption (ECC) mechanism [13], which is proved more efficient than traditional PKI. However, this kind of mechanism needs an additional Certification Authority (CA) to generate user certification. ID-based ([14], [15]) or certificateless based ([16], [17]) mechanisms need also the Networks Manager (NM) to achieve this security function, which are not well suitable for Intra-WBAN communication. Complex parameter assignment and key management are also the major challenges for asymmetric encryption in WBAN.

Another trend is the security scheme based on the physiological signal or channel quality introduced in [18], [19], [20] and [21]. The nodes can use the collected physiological signals to encrypt and decrypt messages. However, the processing of these physiological signals needs additional powerful elements to handle. Because in this case, sensor nodes don't only need to store physiological signals as Data, but also need a further treating of these signals as a part of encryption process. These elements are expensive and consume additional energy. For example, in [18], to use Electrocardiography (ECG) signals, it needs additional device to do Discrete Meyer Wavelet transform (DWT). Also, the distance, the changing of temperature or the human body mobility can make the collected physiological signals different at two different nodes.

More recently, in order to respond to the three challenges of WBAN security, BANZKP [22] and TinyZKP [23] where specifically designed for WBAN and use ZKP based authentication mechanism.

The best to date ZKP-based scheme, BANZKP [22], uses less memory to store private secrets and requires less computing capacity than TinyZKP [23] and the Elliptic Curve Encryption Based Public Key Authentication scheme [13]. BANZKP is also resilient to a wide range of attacks. However, BANZKP still suffers from some specific malicious attacks such as Data Replay attack, DDoS Attack at sink and Redundancy Information Crack. Moreover, the resilience of BANZKP to human body postural mobility in WBAN environment was left as open question.

Our Contribution. In this paper, based on an extensive analyze of the security weakness of BANZKP we propose a new ZKP-based scheme that outperforms

BANZKP from both security and networking point of view. An extended abstract of this paper appear in [24]. Our scheme BAN-GZKP is resilient to Data Redundancy Cracking, Data Replay Attack and DDoS Attack at the sink and optimizes the ZKP exchanging scheme. Furthermore, we stress both BAN-GZKP and BANZKP schemes face to human body postural mobility. When these schemes are plugged to convergecast protocols we prove via extensive simulations that for strategies that use BAN-GZKP scheme outperforms with respect to the case when BANZKP is used. Additionally, our BAN-GZKP scheme presents better computational complexity and less energy consumption than BANZKP while it has the same memory complexity.

Roadmap. The paper is organised as follows. Section 2 presents and overview of the BANZKP scheme and discusses its vulnerabilities. Then, Section 3 presents our new BAN-GZKP, and its security analysis. The resilience of BANZKP and BAN-GZKP face to human body postural mobility when BANZKP and BAN-GZKP are combined with known convergecast strategies, and theirs performances comparison analysis are shown in Section 4. We present, finally, a summary and conclude our work in the Section 5.

2. BANZKP vs Security Attacks

In this section we recall briefly BANZKP [22] (the best to date ZKP-based scheme designed for WBAN), then we analyze its vulnerabilities in terms of resilience to security attacks.

2.1. BANZKP Overview

BANZKP [22] combines a *Zero knowledge Proof* and a *Commitment Scheme*.

The *Zero knowledge Proof* scheme ensures bidirectional authentication between two parties (a sender and a verifier). The idea is by exchanging challenge and response messages between two parties, they can finally trust each other that they hold the same *secret information*, but none of them sent this secret information into the channel during the challenge and response phase. The security level is guaranteed by the fact that it is practically impossible to solve the discrete logarithms for numbers represented on hundreds of bits [23]. In BANZKP the two parties exchange *five challenge/response* messages and never disclose the shared secret.

The *Commitment Scheme* ensures that a sender transmits an encrypted message to a receiver who does not have the decryption key yet. The key is transmitted later as soon as the identity of the receiver is confirmed. In BANZKP, the Commitment Scheme is transmitted directly in plaintext. Because, this key is only used to verifier the identity of the sender and will be used only once per authentication session. So this key is useless after this session and will not give any secret information to anyone.

BANZKP between two nodes N_1 and N_2 executes the following five steps:

$$1) N_1 > ---- E(K_I[ID_{N_1}||V^p]) ----> N_2$$

$$2) N_1 < E(K_I[ID_{N_2}||V^q||RI]), E(K_{CS}[V_{RI}^{p*q}]) < N_2$$

$$3) N_1 > ---E(K_I[ID_{N_1}||V_{RI}^{q*p}]) ----> N_2$$

$$4) N_1 < ------- K_{CS} ---------- < N_2$$

$$5) N_1 > ---E(K_I[ID_{N_1}||DATA]) --> N_2$$

ID_{N_1} and ID_{N_2} are identities of N_1 and N_2 respectively; V is the shared secret number; p and q are two random values generated by N_1 and N_2, respectively; K_I is a shared key between N_1 and N_2; K_{CS} is a random key generated by N_2 for the *Commitment Scheme* and the function $E(K[a])$ means encrypt a with key K. RI is the indicator of the beginning of an interval value of V^{q*p}, represented by V_{RI}^{q*p}. In BANZKP, the size of this interval is 200 bits.

Notice that, V should be a number big enough, and p and q should also randomly chosen to be big enough. So that we can make sure the V^{q*p} has minimal 1096 bits to randomly chose a interval of 200 bits [22].

During the *initialization* phase, both participant nodes store locally a shared secret number V and a shared key K_I by operator (user) manually. Considering the limited number of the nodes in WBAN, manual operations is feasible.

During the *authentication* phase, when a source node has Data packet to send, an authentication session is initiated:

1. N_1 initiates the authentication session. It choses a random value p and computes V^p. It then encrypts his ID and V^p by K_I and sends the whole message to N_2.
2. Upon reception of V^p, N_2 generates a random value q and computes V^q and V^{p*q}. N_2 then

generates a random indicator RI and choses a 200 bits interval value of the V^{p*q} from the indicator RI, as V_{RI}^{p*q} (see Figure 1). N_2 sends back to N_1: (1) ID_{N_2}, V^q and RI encrypted by K_I; (2) V_{RI}^{p*q} encrypted by a random chosen session key K_{CS}.

3. Upon reception of response of N_2, N_1 computes V^{q*p} and uses the received RI to compute V_{RI}^{q*p}. N_1 then sends his ID and V_{RI}^{q*p} encrypted by K_I to N_2. N_1 also keeps $E(K_{CS}[V_{RI}^{p*q}])$ from N_2 and waits the K_{CS} sent later to verify the legitimacy of N_2.
4. Upon reception of V_{RI}^{q*p}, N_2 compares this value with his own value, V_{RI}^{p*q}. If these two values are equal, then N_2 is sure that N_1 has the same shared secret V. Then it confirms the authentication by sending the K_{CS} to N_1. Otherwise, N_2 discards the message and closes the session.
5. Upon reception of K_{CS}, N_1 decrypts $E(K_{CS}[V_{RI}^{p*q}])$ and compares this value with its own value, V_{RI}^{q*p}. If these two values are equal, N_1 is sure that N_2 has the same secret V, and sends ID and $DATA$ encrypted by K_I to N_2. Otherwise, N_1 discards the message and closes the session.

BANZKP copes with the following attacks:

- *Forge Nodes* [22]: Thanks to the bidirectional authentication, any forge node attempting to disguise itself in a legitimate node cannot be certified. This is due to the fact that forge node has no information on the shared secret. Hence, it cannot compute the correct authentication response.

- *Replay Attack* [22]: Adversary could intercept previous exchanged messages and try to use them to make other nodes in the networks trust its identity and finish the bidirectional authentication. The use of randomly chosen p and q makes each authentication session different with respect to the previous ones. Hence, old messages cannot help to correctly execute the authentication.

- *Man in the Middle Attack* [22]: In this attack, the adversary listens channels and try to steal the shared secret. BANZKP does not send directly secret information.

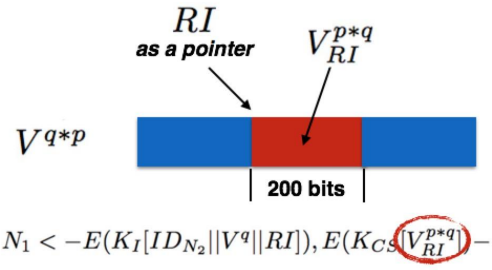

Figure 1: Computing V_{RI}^{p*q}

- *Guessing Attack* [22]: The use of random values for q, p and RI makes practically impossible for the adversary to guess the shared secret value V from V_{RI}^{q*p} or V_{RI}^{p*q}.

- *Privacy Attack* [22]: The adversary may try to eavesdrop. BANZKP prevents this attack by encrypting exchanged Data message with K_I.

2.2. BANZKP vulnerabilities

In this section we analyze the BANZKP vulnerabilities.

Data Replay Attack: BANZKP scheme can prevent malicious authentication message replay by using the random values q, p and RI. However, for encrypting Data message, a constant key K_I is used for all Data message. A conscious adversary may launch a Data Replay Attack by observing the pattern of the exchanges. For example, two nodes are exchanging the authentication messages; an adversary, who holds a captured previous Data message encrypted by K_I from N_1 in previous authentication session between N_1 and N_2, is listening the channel. In the phase 4) of BANZKP, N_2 sends the random key, K_{CS} to N_1. The adversary can also receive this key. At this particular moment, the adversary knows that N_2 is, from now on, waiting for an encrypted Data. The adversary thus sends immediately the previous captured Data message to N_2 to pretend this expired Data message as a fresh one. The consequence is that N_2 treats the expired Data message as the right one and ignores the right message from N_1 and allows the adversary to inject invalid Data into the network.

Redundancy Information Crack: The encryption in BANZKP uses the stream cipher mechanism where each bit of collected Data does the exclusive or with each bit of the encryption key. Since the key used for

Data encryption is always the same K_I at the end of each authentication session, Data messages sent by source nodes have the following format: $M_1 = Data_1$ xor K_I, $M_2 = Data_2$ xor K_I... By capturing M_1 and M_2, the adversary can do the *xor* of them to get redundancy information: M_1 xor $M_2 = Data_1$ xor $Data_2$. After getting enough redundancy information, encrypted Data could be cracked and from the Data, K_I then will be no longer a secret.

DDoS Attack at Sink: BANZKP was designed to work for both single-hop and multi-hop WBAN networks. In multi-hop WBAN environment, BANZKP uses relay nodes to forward the source messages to the sink. From the original BANZKP design, the bidirectional authentication is an end-to-end authentication between the source node and the sink. Relay nodes will just forward the messages. Hence all the authentication or Data information is transparent to them. If an adversary sends continuous invalid authentication request messages (phase 1 of the BANZKP scheme), relay nodes will forward these messages to the sink. The sink will then suffer from a DDoS attack if the amount of the authentication requests is high. The network resources will be consumed by these invalid authentication requests and the real authentication messages get thus less chance to reach the sink.

Potential Adaptation Problem: Intra-WBAN communication is affected by high nodes mobility, the important channel attenuation given by the signal absorption and the reflection of human body. An end-to-end authentication may not be efficient when facing the unstable and high dynamic environments due to packets loss during the multi-hops transmission from sources to the sink. Any loss of timeout during the transmission will lead to the fail of the whole authentication phase.

3. BAN-GZKP

Original BANZKP scheme shows vulnerabilities in terms of security and reliable communications. In this section we present our new BAN-GZKP scheme that improves over BANZKP in several ways. BAN-GZKP is resilient to all the attacks supported by BANZKP plus the Data Replay Attack, Redundancy Information Crack and DDoS attack at sink. Moreover, BAN-GZKP presents better performances in terms of percentage of packets received at the sink, end-to-end delay and the number of transmissions. BAN-GZKP needs only *three phase exchanges* which is optimal in the ZKP class of schemes.

We first present the ingredients that compose our new BAN-GZKP scheme and analyze its resilience attack and its complexity in terms of memory and computation.

3.1. BAN-GZKP Ingredients

In order to tolerate Data Replay Attack, Redundancy Information Crack and DDoS attack at sink BAN-GZKP uses three ingredients: *a random key allocation*, a *hop-by-hop* authentication and the ZKP *Exchanging Schemes Optimization*.

3.1.1. Random Key Allocation

Data Replay Attack and Redundancy Information Crack are possible in BANZKP because a constant key K_I is used to encrypt all Data messages.

An effective and well adapted key management mechanism is necessary to generate different encryption keys for Data messages per session.

The idea of Random Key Allocation is as follows: when nodes authenticate, the shared secret value V^{q*p} will be obligatory computed for each authentication session. Since p and q are randomly chosen, V^{q*p} is also random. During the authentication Phase 4 in the original BANZKP, N_2 will send the random session key to N_1 to decrypt previous information. Notice that, even though K_{CS} is random, this key should not be used to encrypt Data messages because it has been sent on clear text. Our idea is to use K_{CS} as a random pointer that will point to a bit in the binary representation of the random value V^{q*p}. Then we chose an interval in the binary representation of V^{q*p} that starts with the bit pointed by the random pointer K_{CS}. This interval, of length K_{CS} can be seen as a random key, K_R, to encrypt Data message for the current session (see Figure 2).

Our Random Key Allocation does not require additional keys at the initialization and does not need the send of additional fields.

3.1.2. Hop-by-Hop Scheme

Note that Sink-Side DDoS Attack happens in the end-to-end authentication scheme because relay nodes cannot detect whether the authentication message is legal or not. Only the sink can do. To solve this problem and prevent Sink-Side DDoS Attack, we need to

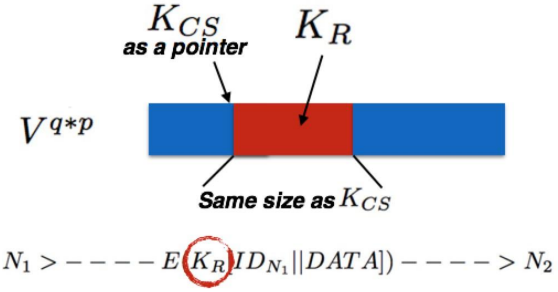

Figure 2: Computing K_R, a Random Data encryption Key

provide relay nodes with the capacity to detect invalid authentications.

The idea is as follows, instead of doing the authentication between the pair source-sink, we let source nodes to initiate authentication directly with their one-hop neighbours. After this authentication phase finishes with success, a source is allowed to send Data messages to the authenticated neighbour. The neighbour who receives Data messages can then initiate authentication with its neighbours until Data reaches to the sink.

An adversary who wants to initiate a large number of invalid authentication requests to block the network will be detected directly by its one-hop neighbours and the DDoS Attack can thus be limited in a local range.

3.1.3. ZKP Exchanging Scheme Optimization

Original ZKP schemes need five-times continuously message exchanging to achieve a bidirectional authentication. This scheme could be optimised to three-times continuously message exchanging under certain conditions. The reduction of the exchanged messages could save network resources, and further improve the total Intra-WBAN performance. The idea of the optimization proposed for BAN-GZKP is as follows:

A) For any authentication exchanging between two nodes who never be authenticated to each other before, we take exactly the same scheme as the original BANZKP to do the bidirectional authentication.

B) When a source node N_1 initiates authentication with another node N_2 that previously authenticated with N_1 and that recognizes the identity of N_1, we can then optimise the total authentication scheme to the following:

$$1) N_1 > - - - - - E(K_I[ID_{N_1}||V^p]) - - - - - > N_2$$

$$2) N_1 < - - E(K_I[ID_{N_2}||V^q||RI||R||V_{RI}^{p*q}]) - - < N_2$$

$$3) N_1 > - - - - E(K_R[ID_{N_1}||DATA]) - - - - > N_2$$

When a source node has Data packet to send, an authentication session is initiated:

1. N_1 initiates the authentication session. It choses a random value p and computes V^p. It then encrypts its ID and V^p by K_I and sends the whole message to N_2.
2. N_2 recognizes the identity of N_1, then N_2 instead of sending back $E(K_I[ID_{N_2}||V^q||RI])$, $E(K_{CS}[V_{RI}^{p*q}])$, where V_{RI}^{p*q} is encrypted with K_{CS} (as in original BANZKP scheme), it sends back directly V_{RI}^{p*q} encrypted with the initial key K_I. In our BAN-GZKP N_2 needs just to send a random pointer R for the Random Key Allocation. Hence, the final message sent back to N_1 is: $E(K_I[ID_{N_2}||V^q||RI||R||V_{RI}^{p*q}])$.
3. After receiving the response of N_2, N_1 finishes the authentication using the same mechanism, and choses a random key, K_R, from the pointer R of Random Key Allocation and encrypt Data by K_R then sends the message to N_2, if V_{RI}^{p*q} and V^{q*p} are equal. We thus can complete the authentication session after the first successful authentication between these two nodes. If not, N_1 discards the message and closes the session.

3.2. BAN-GZKP Security Analysis

BAN-GZKP reduces the number of authentication messages and also tolerates the attacks tolerated by BANZKP scheme. Additionally it tolerates Data Replay Attack and Redundancy Information Crack. As for the case of BANZKP, BAN-GZKP can be implemented either end-to-end or hop-by-hop. Note that BAN-GZKP hop-by-hop scheme is also resilient to Sink-Side DDoS Attack.

Inspired by [25], we propose formal security proof of BAN-GZKP. We first define a node A hold S as node A known information is:

$$I_A = \{S\} \tag{1}$$

Let the operation of sending a message including X as content of the message from node A to node B at ith authentication phase is:

$$A : (A, X, B)_i, \quad i \in \overline{1,5} \tag{2}$$

In BAN-GZKP, for the first time of the authentication, we need total five authentication phases (each

authentication message exchange is seen as a authentication phase), but form the second time of the authentication between these two nodes, it's need only three authentication phases. Let the Checking operation of a legitimate (honest) node A to verifier a received message from B is legal or not is:

$$Checking_A((B, X, A)_i) \quad (3)$$

If message $(B, X, A)_i$ can not be decryption correctly or X can not is not the correct response of previous challenge, then the Checking operation failed, node drop the received message. If not, Checking succeeded, then node continues the next authentication exchange.

Let's define a node Z as a smart adversary, who apply operations as following:

- Z can intercept the message sent form A to B at any authentication phase.
- Z can initiate an authentication message: $Z : (A, X, B)_i$ where A and B can be any nodes in the network, and X can be anything belonging to I_Z.
- Z can don't check any message and confirm arbitrarily that checking failed or succeeded.
- Z can update I_Z, when intercepting message.
- Z can try to decrypt encrypted message by using information from I_Z at any time.

In the following, we prove that BAN-GZKP is tolerant to the adversary Z defined above.

Proposition 1. BAN-GZKP is resistant to Forge Nodes Attack.

Proof Let Z is a Forge Nodes attempting to disguise itself in a legitimate node to authenticate with B. The initial information of Z and B is:
$I_Z = \{ID_Z, ID_B, K_{I_Z}, V_Z, p\}$
$I_B = \{ID_B, K_{I_B}, V_B\}$
And following the operations shown below, Z can not authentication succeed with B.
1) $Z : (Z, E(K_{I_Z}[ID_Z||V_Z^p]), B)_1$
2) $Checking_B((Z, E(K_{I_Z}[ID_Z||V_Z^p]), B)_1)$
3) $Checking\ Failed : K_{I_Z} \neq K_{I_B}$
As Z has only information about the ID of B and itself, Z can not pretend to be a legitimate node, because the message encryption key K_{I_Z} is chosen arbitrarily, B can not decrypted correctly, the checking will fail. As the sender node will always do the authentication with the receiver node; the receiver node does also the authentication with sender node only the first time. In this case, even though the adversary can disguise itself in a legal node A who previously finished the authentication with the receiver B. Because this message sent by this adversary cannot be decrypted correctly.

Proposition 2. BAN-GZKP is resistant to Authentication Replay Attack.

Proof The proof decomposes in two parts. In the first parts, let Z intercept a message $(A, X, B)_1$. Then Z can replay directly this message to disguise itself in a the node A who previously finished the authentication with B. The initial information of Z and B are:
$I_Z = \{ID_Z, ID_A, ID_B, (A, X, B)_1, K_{R_Z}\}$
$I_B = \{ID_A, ID_B, K_{I_A} = K_{I_B}, V_A = V_B, K_{R_B}\}$
Following the operations shown below, B can detected the message is a replay message.
1) $Z : (A, X, B)_1$
2) $Checking_B((A, X, B)_1)$
3) $Checking\ Succeeded : K_{I_A} = K_{I_B}, V_A = V_B$
4) $B : (B, E(K_{I_B}[ID_B||V_B^q||RI||R||V_{RI}^{p*q}]), A)_2$
5) $Z\ intercepts\ (B, E(K_{I_B}[ID_B||V_B^q||RI||R||V_{RI}^{p*q}]), A)_2$
6) $Z\ confirm\ Checking\ Succeeded$
7) $Z : (A, E(K_{R_Z}[ID_A||DATA]), B)_3$
8) $Checking_B((A, E(K_{R_Z}[ID_A||DATA]), B)_3)$
9) $Checking\ Failed : K_{R_Z} \neq K_{R_B}$
Even though B trusts the replay message, the Data message encrypted with the wrong encryption key K_{R_Z} will be detected by B at the end of the authentication phase.

In the second part, we assume that the adversary tries to replay the message sent by B in phase 2, and try to get information from A, the initial information of Z and A are:
$I_Z = \{ID_Z, ID_A, ID_B, (B, X, A)_2\}$
$I_A = \{ID_A, ID_B, K_{I_A} = K_{I_B}, V_A = V_B\}$
Following the operations shown below, this message will directly drop since p chosen by A are different random values for each session, a replay message can not pass the checking at A.
1) $A : (A, E(K_{I_A}[ID_A||V_A^p]), B)_1$
2) $Z\ intercepts\ (A, E(K_{I_A}[ID_A||V_A^p]), B)_1$
1) $Z : (B, X, A)_2$
2) $Checking_A((B, X, A)_2)$
3) $Checking\ Failed : V_{RI}^{p*q}\ computed\ from\ A\ is\ different\ from\ V_{RI}^{p*q}\ received\ from\ X$

Notice that, we cannot simplify the authentication at A. Otherwise, the adversary can replay the same message from B, to force A to use the same key K_R to encrypt the Data message. Hence, the adversary can later initiate a Redundancy Information Crack.

Proposition 3. BAN-GZKP is resistant to Man in the Middle Attack and Guessing Attack.

Proof Z can intercept messages exchanged between A and B as a Man in the Middle to try Guessing secret value V hold in A and B, The initial information of Z is: $I_Z = \{ID_Z, ID_A, ID_B\}$
Following the operations shown below, Z can not get any useful information to decrypt message and Guess the content of Data message.
1) $A : (A, X_1, B)_1$
2) $B : (B, X_2, A)_2$
3) $A : (A, X_3, B)_3$
...
x) Z *update* I_Z
$x+1$) $I_Z = \{ID_Z, ID_A, ID_B, X_1, X_2, X_3...\}$
$x+2$) Z *try decrypt messages to get* V
The attempting of decryption will fail because none of information in $I_Z = \{ID_Z, ID_A, ID_B, X_1, X_2, X_3...\}$ contain the secret number V.

Proposition 4. BAN-GZKP is resistant to Data Replay Attack.

Proof Z can replay a Data messages from A and B, and make B think the replay message is correctly message. The initial information of Z and B are:
$I_Z = \{ID_Z, ID_A, ID_B, (A, X, B)_3\}$
$I_A = \{ID_A, ID_B, K_{I_A} = K_{I_B}, V_A = V_B\}$
Following the operations shown below, the replay message will directly drop. Since in each session, K_R is different, message encrypted by K_R computed from other session can not be decrypted correctly by B:
1) $Z : (A, X, B)_3$
2) $Checking_B((A, X, B)_3)$
3) $Checking\ Failed : K_R$ *computed from* B *can not decrypt* $(A, X, B)_3$

Proposition 5. BAN-GZKP is resistant to Redundancy Information Crack.

Proof Z can intercept encrypted Data messages sent from A and B, and make try to decrypt Data message. The initial information of Z is:
$I_Z = \{ID_Z, ID_A, ID_B\}$
Following the operations shown below, Z can not get Data information from collecting Redundancy Information of encrypted Data messages.
1) $A : (A, X_1, B)_3$
2) $A : (A, X_2, B)_3$
3) $A : (A, X_3, B)_3$
...
x) Z *update* I_Z
$x+1$) $I_Z = \{ID_Z, ID_A, ID_B, X_1, X_2, X_3...\}$
$x+2$) Z *try decrypt messages to get* V
As X_i is the Data information encrypted by K_R and in each authentication session, K_R change randomly. Z can not get Data information from Redundancy Information of encrypted Data message.

Proposition 6. BAN-GZKP is resistant to DDoS attack at sink.

Proof a Z may continue send message into its neighbour node to lance a DDoS attack at the sink by let neighbour node forwarding these message to the sink. The initial information of Z and B is:
$I_Z = \{ID_Z, ID_B\}$
Following the operations shown below, all the useless transmission initialed from Z will be blocked at B.
1) $Z : (Z, X, B)_1$
2) $Checking_B((Z, X, B)_1)$
3) $Checking\ Failed : B$ *can not decrypt* $(Z, X, B)_1)$
As $(Z, X, B)_1$ failed the checking at B, this message will be dropped directly. B thus prevent the DDoS broadcasting into the whole network.

3.3. Memory and Computational Complexity and Energy Consumption

In [22], authors prove that BANZKP improves over existing similar schemes in terms of memory requirements, computation complexity and energy consumption. In the following we study the costs of BAN-GZKP compared to BANZKP. In terms of the parameters required to be stored by each node for the initial phase, both the end-to-end and hop-by-hop BAN-GZKP need that source nodes and the sink store the shared value V and the initial key K_I. Hence, BAN-GZKP has the same memory complexity as the original BANZKP.

In terms of *computational complexity*, a complete authentication phase in the original BANZKP requires four times big number multiplications and five times encryption/decryption. Our BAN-GZKP scheme requires four times big number multiplications, but only

three times encryption/decryption. Our scheme presents a better computation complexity for each complete authentication phase.

In terms of *energy consumption*, the original BANZKP needs five transmission phases for a complete authentication. Even though our optimal scheme sends an additional field, R as a random pointer in exchange phase number 2), BAN-GZKP needs only three transmission phases instead of five. The energy needed to send the R value is hence negligible compared to two complete transmissions of BANZKP.

To sum up, the new BAN-GZKP scheme optimizes BANZKP by adding a Random Key Allocation mechanisms and a Hop-By-Hop authentication. Moreover BAN-GZKP has better computational complexity and energy consumption than BANZKP.

4. Analysis of Resilience to Postural Mobility

In the following we analyze the effectiveness of BANZKP and BAN-GZKP schemes face to postural mobility. We therefore consider as case study the convergecast problem where Data messages sent by source nodes are collected by a specific node in the network called sink. We enrich representative convergecast strategies specifically designed for multi-hop WBAN mentioned in [26] and [27] with BANZKP and BAN-GZKP schemes, respectively. Note that the original BANZKP scheme requires an end-to-end authentication where all the authentication messages are transparent to relay nodes. Only the source and the sink can understand these messages; BAN-GZKP is a Hop-By-Hop authentication scheme, where source nodes initiate authentication with their one hop neighbours. If these nodes are chosen to relay Data messages then before relaying these messages they apply the hop-by-hop authentication with their neighbours.

We evaluate the performances of both BANZKP and BAN-GZKP when these schemes are used in a secure convergecast process. Our evaluation focuses the percentage of packets received at sink for various rates of transmissions and various postural mobilities.

In the next section we briefly present the convergecast strategies we evaluate and the way we plugged the BANZKP and BAN-GZKP schemes to these strategies. Then we discuss our simulation results.

4.1. Convergecast Strategies

In [26] and [27], authors classify existing convergecast strategies for WBAN into five classes: Multi-Paths based Strategies, Tree-based Strategy, Dynamic Path Strategies, Gossip-based Strategies and Attenuation-based Strategies. In our study we plug the BANZKP scheme on five different convergecast strategies (one representative per class).

- *Multi-Paths based Strategies:* are based on pre-determined paths and use these overlay paths as a reliability mechanism. An example is *All Parents to All Parents* (APAP) strategy [26]. In APAP, each source node sends a message to maximum two pre-determined parents. Each parent then forwards received messages to maximum two of their parents.

- *Tree-based Strategy:* [27] pre-constructs seven Best-Path Trees for different human postures shown in Figure 3. Source nodes send messages through these paths to the sink. The pre-constructed Best-Path Trees are computed according to random attenuation distribution of each links.

- *Dynamic Path Strategies:* construct and update a tree-based overlay. The Collection Tree Protocol (CTP) [28] is an example of this class. In CTP each node sends additional BEACON messages to update the overlay route from each source to the sink.

- *Gossip-based Strategies:* use flooding. In this class we choose FloodToSink [26], where a source diffuses messages to all its neighbours, then continue to forward messages to all their neighbours and so on. In this case, every packet has a parameter, Time to Life (TTL), to limit the number of forwarding.

- *Attenuation-based Strategies:* these strategies are based on the negotiation of the channel attenuation. When a source has packets to send, it broadcasts first a Request (REQ) to ask an estimate attenuation from the receiver to the sink. The receiver of the Request will then send back a Reply (REP) with the required estimate attenuation value. The source will chose the next hop among replying nodes and sends data packets to the chosen one. In this class we investigate strategy MiniAtt [26]. This strategy choses one node who has the minimal estimate attenuation to the sink; if no Reply has been received for a while, the source will re-send the Request.

In our simulations we use five strategies to represent each class of convergecast strategies: APAP for Multi-Paths based Strategies; FloodToSink for Gossip-based Strategies; MiniAtt for Attenuation-based Strategies; CTP for Dynamic Path Strategies and Tree-based Strategy to represent itself.

4.2. How BANZKP and BAN-GZKP plugg to convergecast strategies

We explain in Section 4.2.1 and 4.2.2, how BANZKP and BAN-GZKP schemes can be plugged to the WBAN convergecast strategies, respectively. The general idea is that before each source node sends any Data packet, it needs to do the authentication with the sink in the BANZKP or with the next hop in the BAN-GZKP, respectively.

4.2.1. Convergecast with BANZKP

In the authentication phase of BANZKP, source nodes need to exchange an authentication message with the sink. However as original convergecase strategies care about only how to flow authentication messages and Data messages from source to the sink (up stream), we need to define how messages flow from the sink down to the source (down stream). In APAP, CTP and Tree-based strategies, messages generated by the sink will follow the opposite route with respect to the up stream exchanges. That is, parents forward messages to their sons until messages reach the sources.

For MiniAtt strategy, for both up stream and down stream, nodes always need from their neighbours attenuation information in order to chose the next hop. The difference is that for up stream, nodes ask the attenuation between the receiver and the sink; for down stream, nodes ask the attenuation information between the receiver and the initial source.

For FloodToSink there is no difference between the up stream and the down stream.

4.2.2. Convergecast with BAN-GZKP

In BAN-GZKP, there is only up stream for Data from the source to the sink, since nodes only authenticate with their one hop neighbours. After the authentication, nodes send Data messages to the authenticated neighbour. So there is no authentication flow during the transmission, only the Data message will be forwarded from the source to the sink as up stream.

Note that, for APAP and FloodToSink, there is always a multi-receiver when a source initiates the authentication. Receivers will reply to the source, the source then continue the authentication exchanging with all of them. But only the neighbour who finished the authentication phase firstly can be chosen as the legal next hop to avoid additional Data message and to respect the original convergecast strategy.

For MiniAtt strategy, the BAN-GZKP scheme can be integrated into the original Attenuation Require-Response scheme as follows: after a source chooses the next hop it begins to initiate the authentication directly with the chosen node.

For CTP and Tree-based strategies, there is only one parent to forward messages. Hence, the authentication is initiated by nodes with their parents.

4.3. Channel and Human Mobility Model

The WBAN model we used in our research is proposed in [29]. They implement the realistic channel model proposed in [3] over the physical layer implementation provided by the Mixim framework [30], who provides several extensions of existing simulation frameworks specified for wireless and mobility simulation. This channel model of an on-body $2.45\,GHz$ channel between 7 nodes, that belong to the same WBAN, uses small directional antennas modeled as if they were $1.5cm$ away from the body. Nodes are assumed to be attached to the human body on the head, chest, upper arm, wrist, navel thigh, and ankle. In the convergecast strategies we consider six source nodes to send Data as follows: 0) navel, 2) head, 3) upper arm, 4) ankle, 5) thigh and 6) wrist, and one sink node that collects Data, node 1) chest.

Nodes positions are calculated in 7 postures: walking (walk), running (run), walking weakly (weak), sitting down (sit), wearing a jacket (wear), sleeping (sleep), and lying down (lie). Figure 3 shows the positions of sensor nodes change with human mobility human postures within a time period in different postures model [3]. In each posture, a continuous human action has been device into many frames. Each single human body picture with a corresponding frame number, x, in a posture is a screenshot of this continuous human action at the xth frame. For example, in posture 1 Walking, the continuous action takes 30 frame, and in the Figure 3, it shows four screenshots at 1st frame, 10th frame, 20th frame and the 30th frame, respectively. The red diamonds in the figures

represent sensors on the human body moving with the human mobility.

Channel attenuations are calculated between each couple of nodes for each of these positions as the average attenuation (in dB) and the standard deviation (in dBm). The model takes into account: the shadowing, reflection, diffraction, and scattering by body parts. Naganawa et al. [3] studied a cooperative transmission scheme: two-hop relaying scheme. Using the simulated path loss, the performance of such scheme were evaluated by comparing the outage probability using different relay nodes against a direct link between a source and a destination. They advocate for the use of multi-hops communication which has the additional feature that it significantly decreases the transmission power. We thus interested in the network performance when applying BANZKP and BAN-GZKP in different multi-hops on-human communications.

4.4. Simulation Results

In order to evaluate the strategies described above in a realistic WBAN scenario, we implemented them under the OMNeT++ simulator enriched with the Mixim project [30] that specifically models the lower network WBAN layers.

We use standard IEEE 802.15.4 protocol as MAC layer. Note that the most recent standard IEEE 802.15.6 proposed for WBAN considers a star network topology (one hop) and does not take into account the human body postural mobility. As stressed in the introduction we focus multi-hop networks and human body postural mobility.

We consider the following packet rates at the application layer: 1 packet/second, 5 packets/second and 10 packets/second. These values are commonly used in WBAN [31]. The sensibility of WBAN devices is -100dBm and the transmission power has been set to -60dBm. We stress the studied strategies under a realistic channel model and postural mobility as described above.

We evaluated WBAN performance for each studied convergecast strategy under all seven mobility postures, in term of ratio of packet reception rate, data end-to-end delay and also numbers of transmissions plugged with BANZKP and BAN-GZKP, respectively. Figures from 4 to 93 show network performance in different strategies. In each figure, the red columns represent the original convergecast strategies without applying any authentication scheme; the

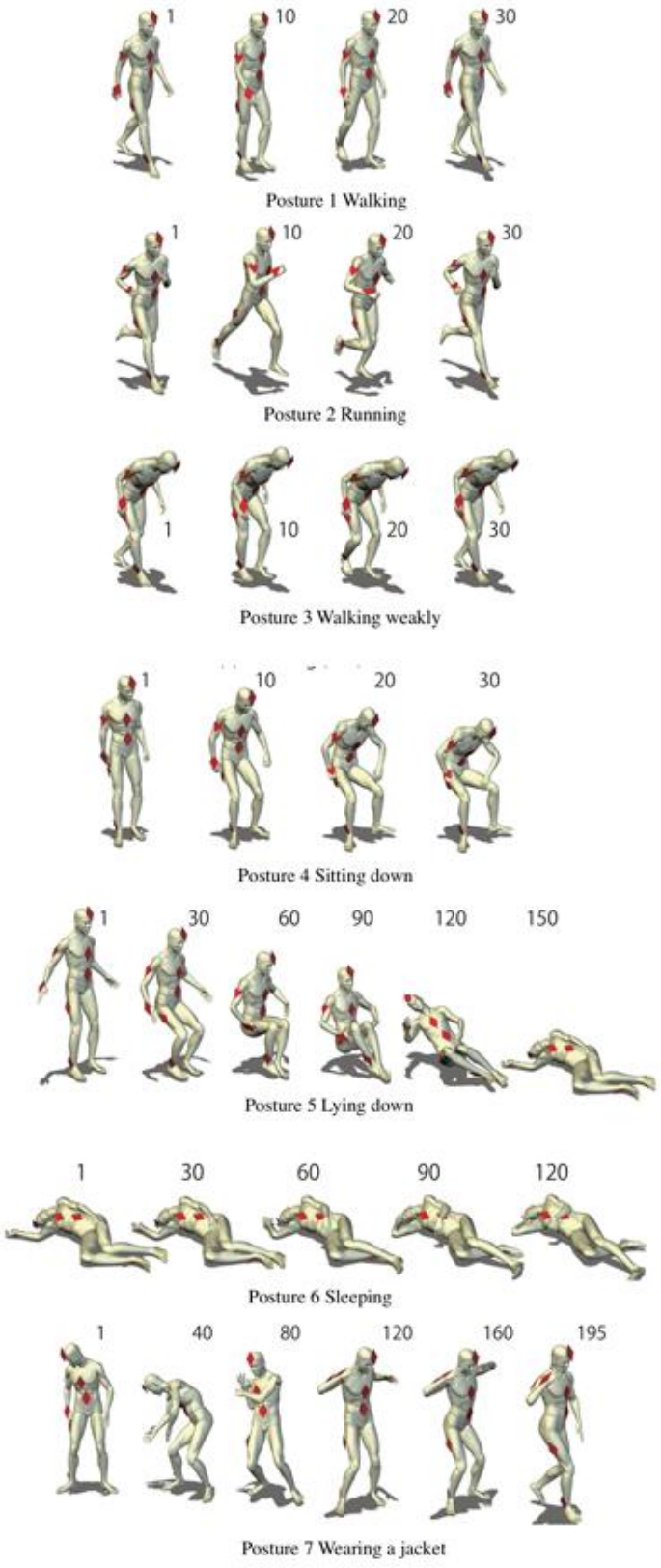

Figure 3: 7 Different Human Postures [3]

white columns represent original strategies applying BANZKP; and the blue columns original strategies applying BAN-GZKP. The vertical bars of each column in figures refer to the confidence intervals. Results computed from 200 runs of simulations observation samples. The confidence intervals β is calculated as:

$$\beta = t(\alpha, R-1) \cdot \frac{S}{\sqrt{R}} \tag{4}$$

where α is 0.005, means the confidence level is 95%, R is the number of observation samples and the S is the standard deviation of observation samples.

For *APAP* strategy (see Figures from 4 to 24, a example for posture 1 Walking), by plugging ZKP scheme into the original APAP strategy, the WBAN performance decreases in general: lower ratio of packets reception, higher end-to-end delay and number of the transmissions, due to the additional ZKP authentication scheme added to the original one. When focusing on the comparison between BANZKP and BAN-GZKP, we noticed that BAN-GZKP has higher ratio of reception, lower end-to-end delay and number of transmissions in all the postures except the number of transmissions in the Posture 6 Sleeping, see Figure 23, where BANZKP has fewer number of transmissions than BAN-GZKP. In Posture 6, links between the nearby nodes to the sink may have important channel attenuations due to the obstruction and reflection of human body when sleeping [27]. Links who are far away from the sink affected by lower attenuations comparing with links who are close to the sink. In the case of the hop-by-hop BAN-GZKP, data packet has a big chance to be lost when reaching these links close to the sink. That means BAN-GZKP may waste all transmissions of hop-by-hop authentication before the data is finally lost. However in the BANZKP case, there is no transmission wasted, since once the authentication packet is lost, after the timeout, the source node will notice the loss and close this transmission session. The BANZKP thus is better in terms of number of transmissions in Posture 6 Sleeping.

For *CTP* strategy (see Figures from 25 to 45, a example for posture 1 Walking), we noticed that the performance parameters have the same behaviour as shown in strategy APAP. BAN-GZKP has better performances than BANZKP in terms of ratio of packets reception, end-to-end delay and number of transmissions except the number of transmissions in Posture

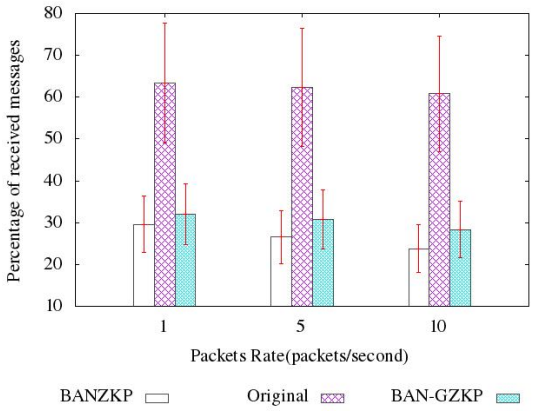

Figure 4: Percentage of received messages for APAP in posture 1

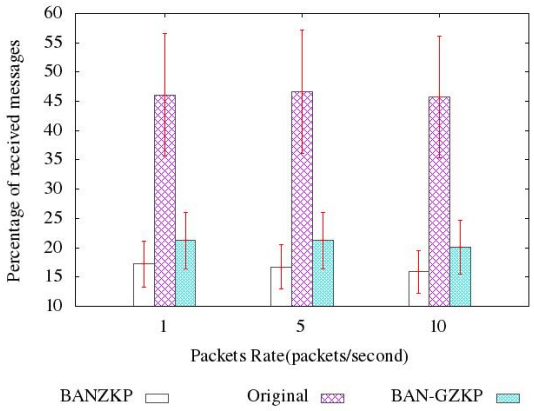

Figure 5: Percentage of received messages for APAP in posture 2

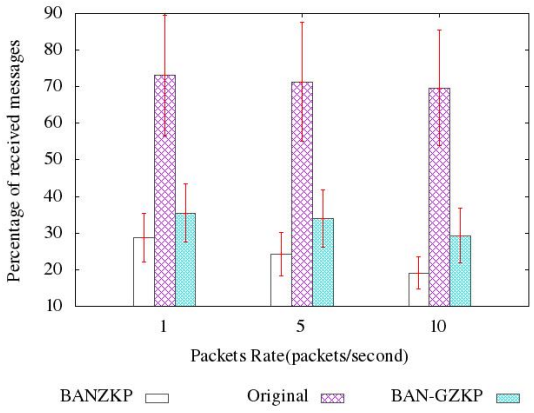

Figure 6: Percentage of received messages for APAP in posture 3

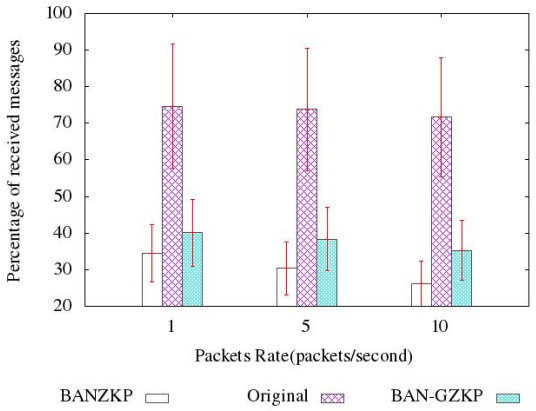

Figure 7: Percentage of received messages for APAP in posture 4

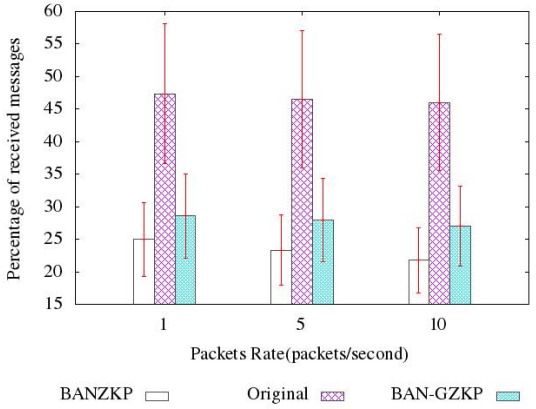

Figure 8: Percentage of received messages for APAP in posture 5

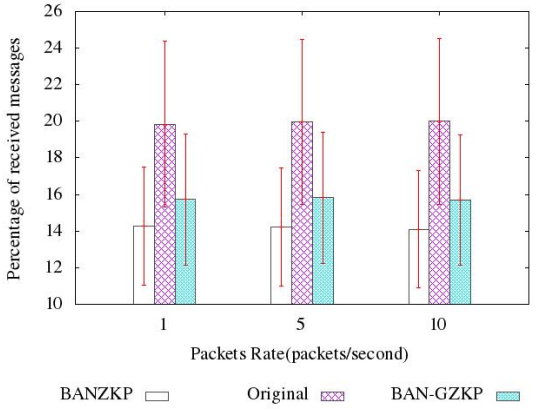

Figure 9: Percentage of received messages for APAP in posture 6

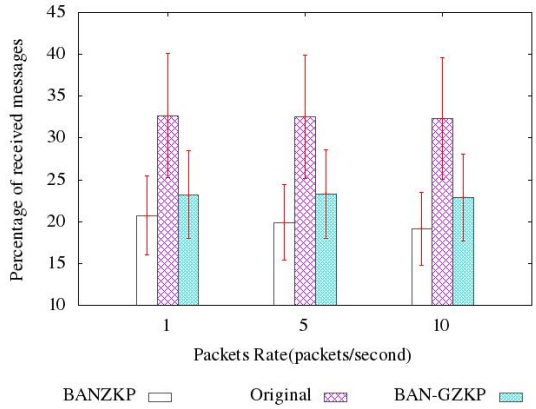

Figure 10: Percentage of received messages for APAP in posture 7

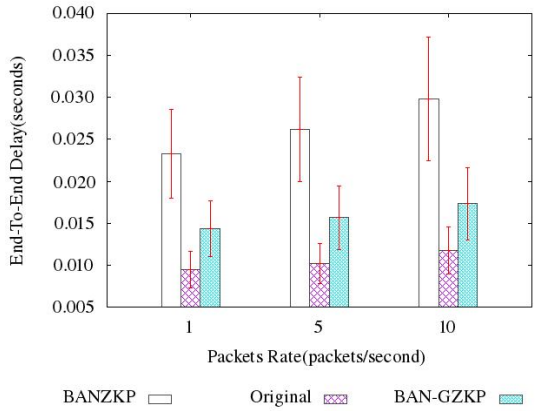

Figure 11: End-To-End Delay for APAP in posture 1

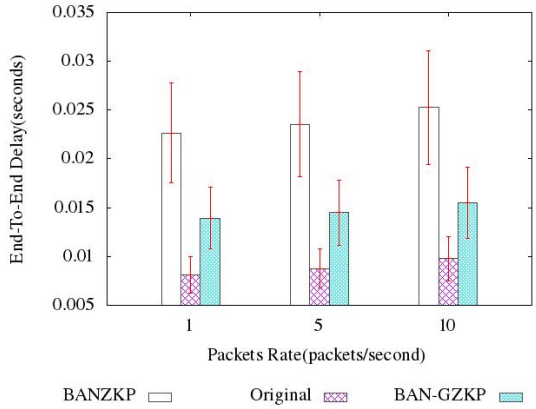

Figure 12: End-To-End Delay for APAP in posture 2

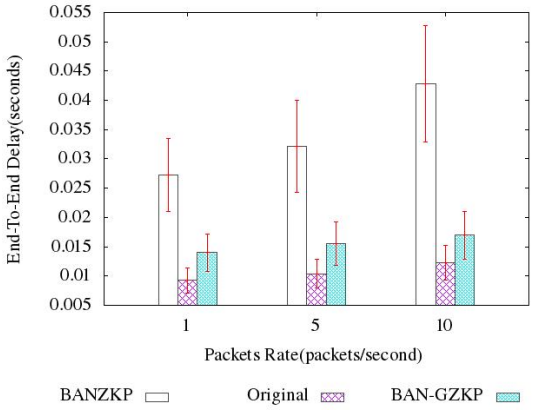

Figure 13: End-To-End Delay for APAP in posture 3

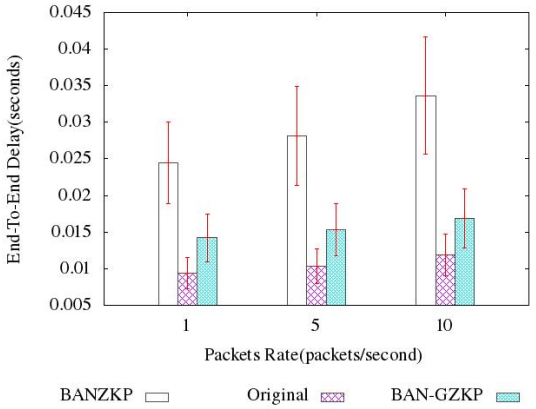

Figure 14: End-To-End Delay for APAP in posture 4

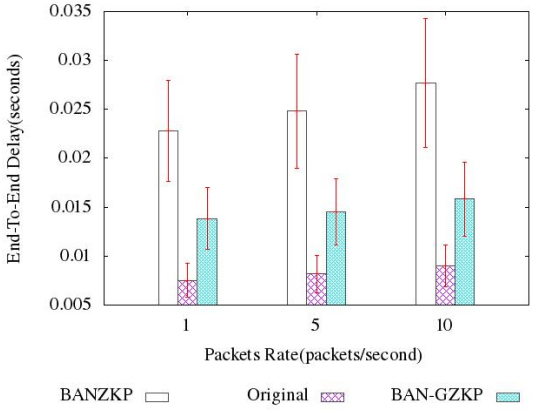

Figure 15: End-To-End Delay for APAP in posture 5

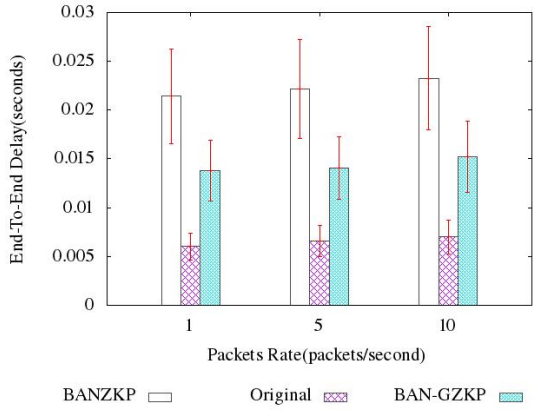

Figure 16: End-To-End Delay for APAP in posture 6

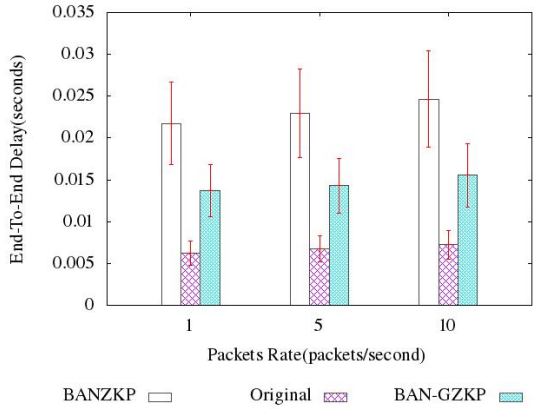

Figure 17: End-To-End Delay for APAP in posture 7

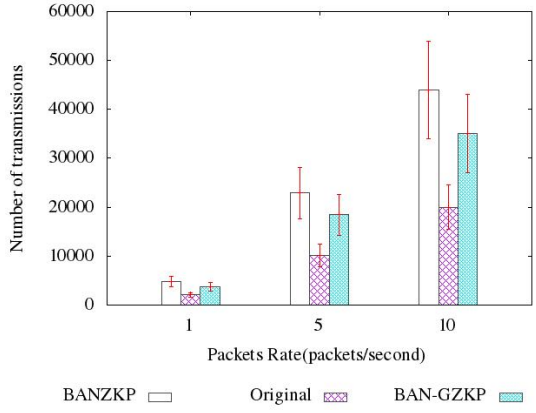

Figure 18: Number of transmissions for APAP in posture 1

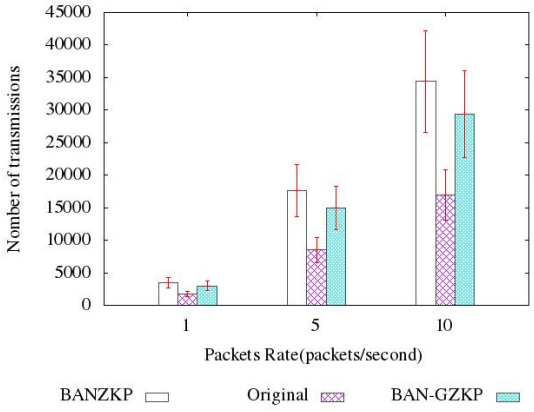

Figure 19: Number of transmissions for APAP in posture 2

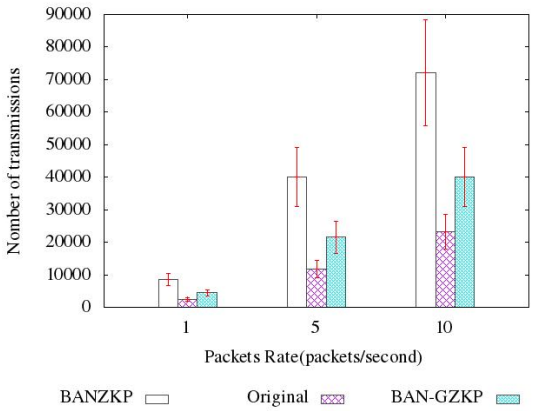

Figure 20: Number of transmissions for APAP in posture 3

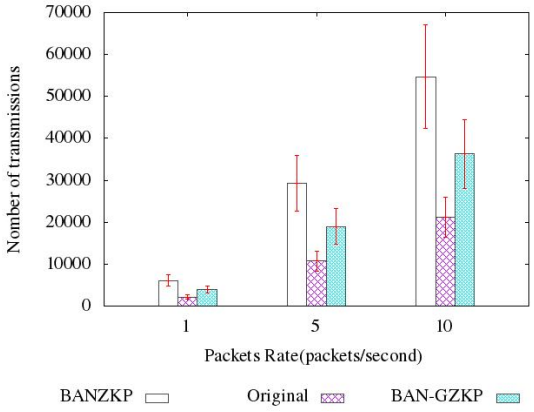

Figure 21: Number of transmissions for APAP in posture 4

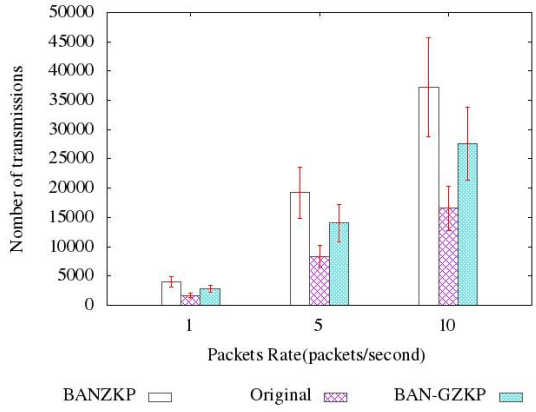

Figure 22: Number of transmissions for APAP in posture 5

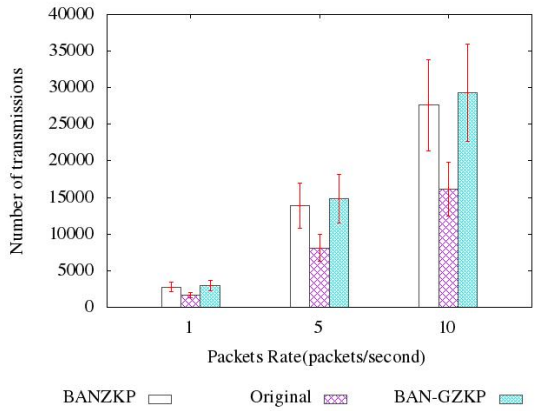

Figure 23: Number of transmissions for APAP in posture 6

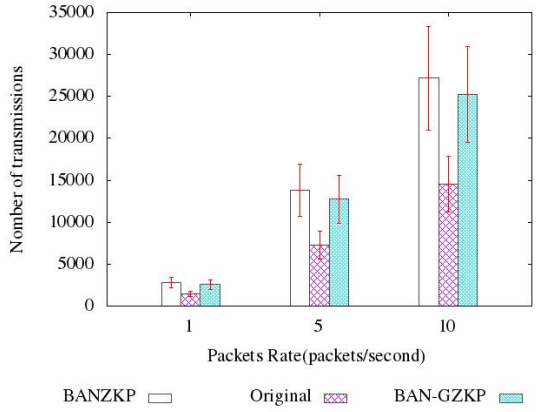

Figure 24: Number of transmissions for APAP in posture 7

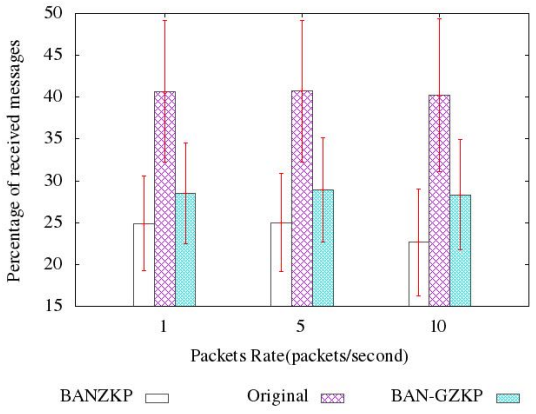

Figure 25: Percentage of received messages for CTP in posture 1

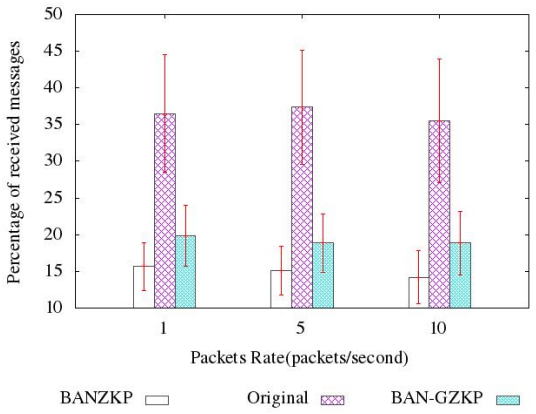

Figure 26: Percentage of received messages for CTP in posture 2

6 Sleeping, see Figure 44. The reason is the same as for the strategy APAP: BAN-GZKP may waste more transmissions than BANZKP before a packet gets lost if the link error occurs near the sink. The reason why BANZKP and BAN-GZKP have the same behaviour in both CTP and APAP, respectively is as follows: CTP constructs a tree from each source node to the sink at the initial phase and keeps updating the tree during the transmission; APAP on the other side uses and keeps pre-setted multiple-reception paths. The common point is that both CTP and APAP tend to maintain good routes from sources to the sink. When a node has a packet to send, it can directly send the packets to an already-keep-in-mid next hop.

For *MiniAtt* strategy (see Figures from 46 to 66, a example for posture 1 Walking), we get lower end-to-end delay and number of transmissions when using BANZKP and BAN-GZKP than the original Mini-Att strategy. That is due to the negotiation nature of MiniAtt strategy: before any transmission, sender

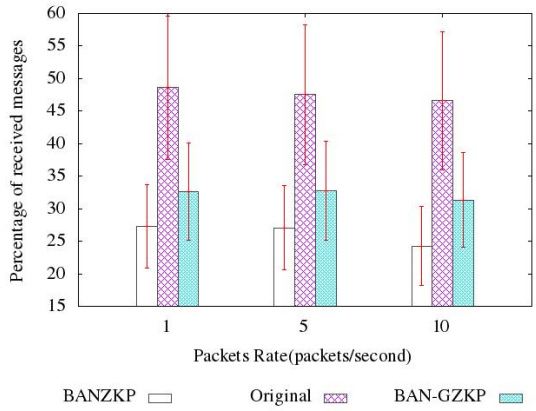

Figure 27: Percentage of received messages for CTP in posture 3

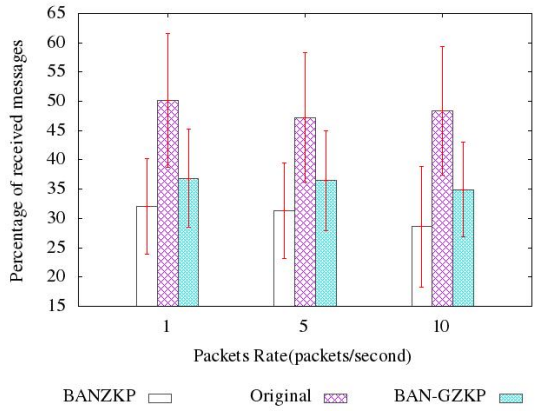

Figure 28: Percentage of received messages for CTP in posture 4

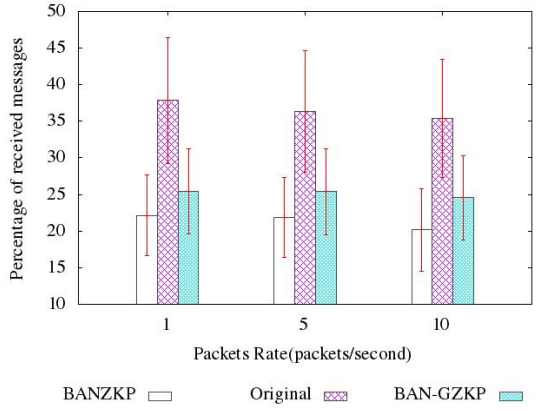

Figure 29: Percentage of received messages for CTP in posture 5

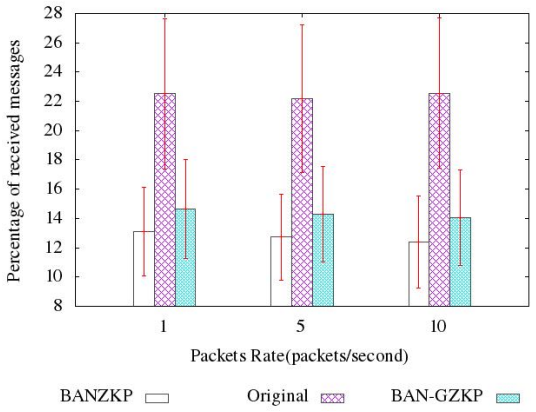

Figure 30: Percentage of received messages for CTP in posture 6

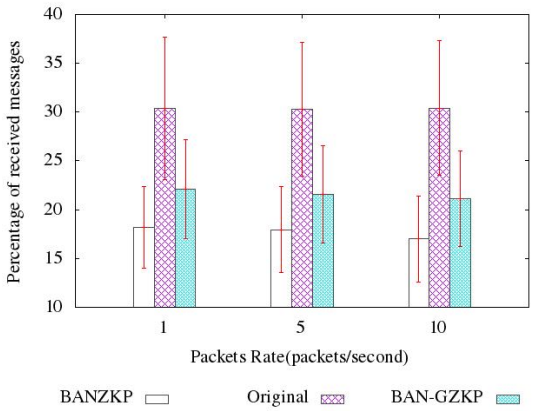

Figure 31: Percentage of received messages for CTP in posture 7

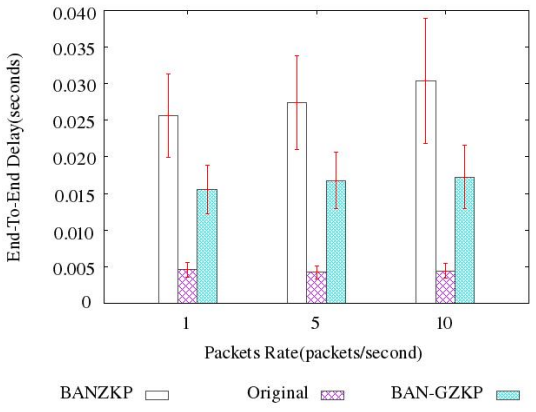

Figure 32: End-To-End Delay for CTP in posture 1

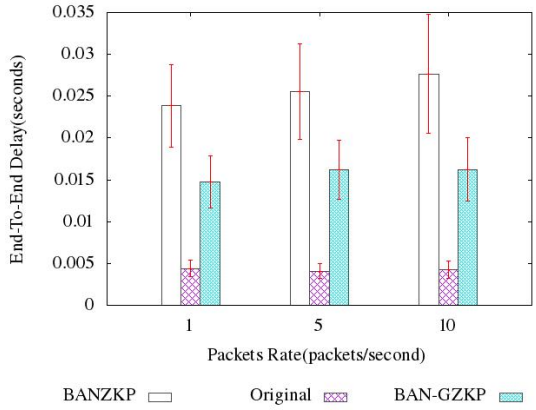

Figure 33: End-To-End Delay for CTP in posture 2

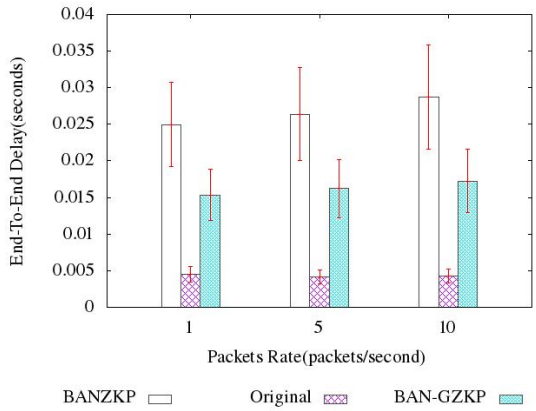

Figure 34: End-To-End Delay for CTP in posture 3

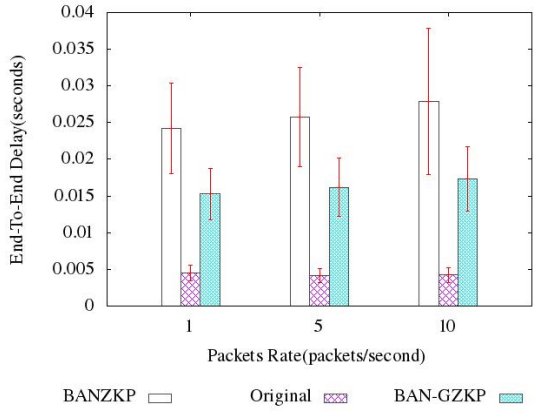

Figure 35: End-To-End Delay for CTP in posture 4

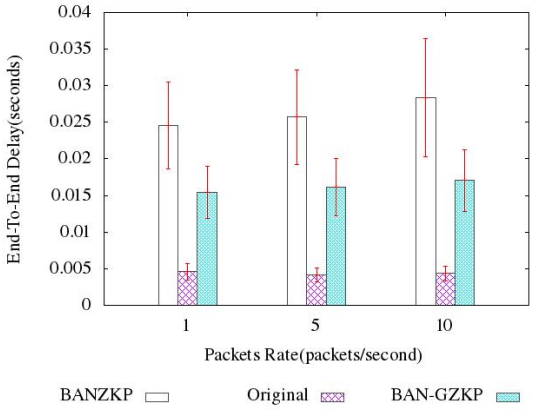

Figure 36: End-To-End Delay for CTP in posture 5

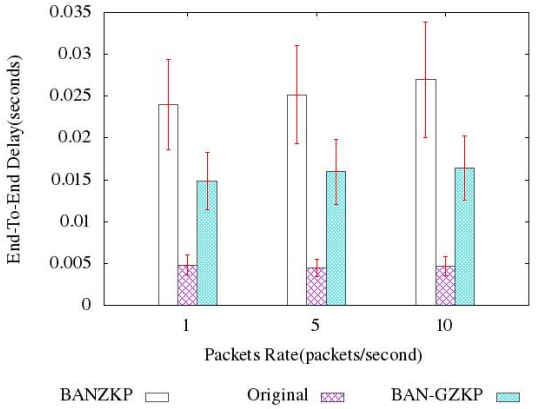

Figure 37: End-To-End Delay for CTP in posture 6

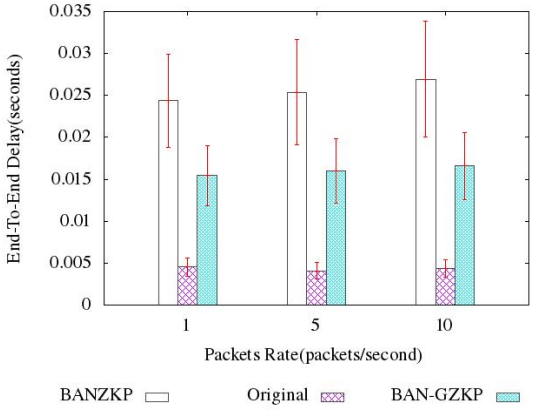

Figure 38: End-To-End Delay for CTP in posture 7

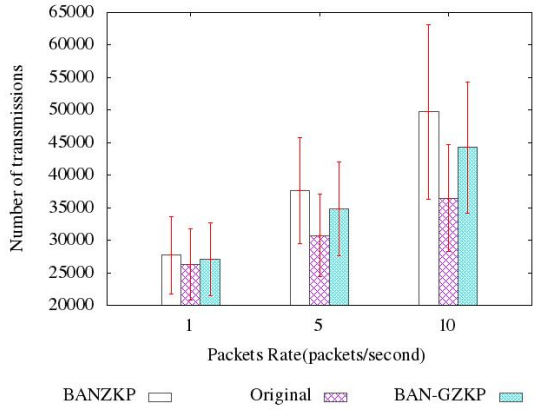

Figure 39: Number of transmissions for CTP in posture 1

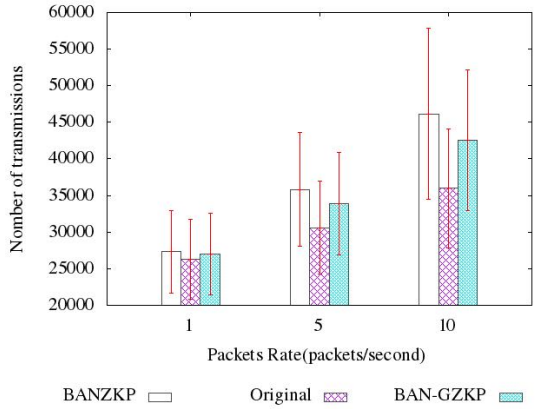

Figure 40: Number of transmissions for CTP in posture 2

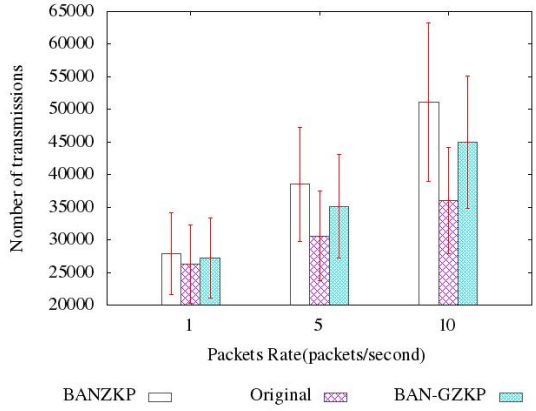

Figure 41: Number of transmissions for CTP in posture 3

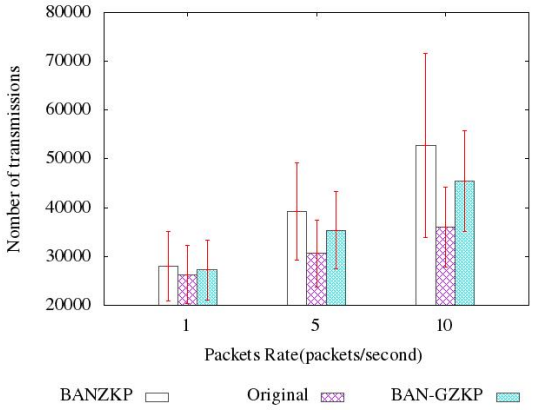

Figure 42: Number of transmissions for CTP in posture 4

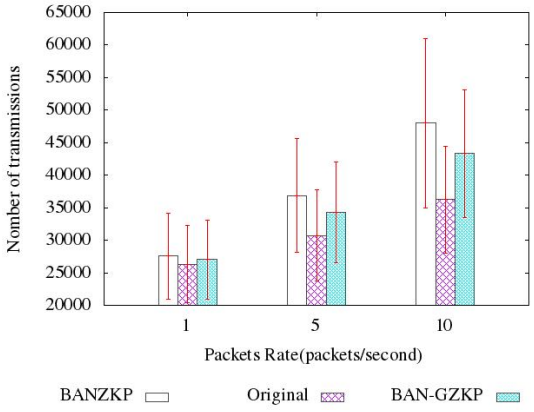

Figure 43: Number of transmissions for CTP in posture 5

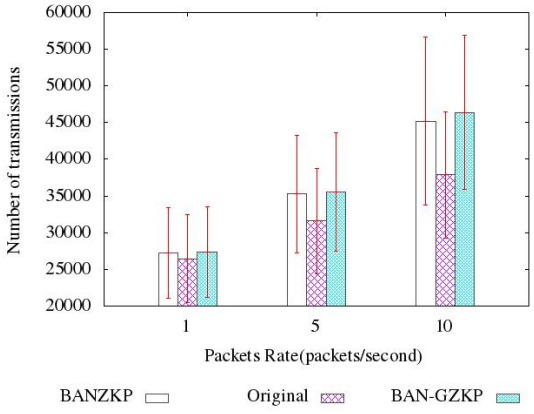

Figure 44: Number of transmissions for CTP in posture 6

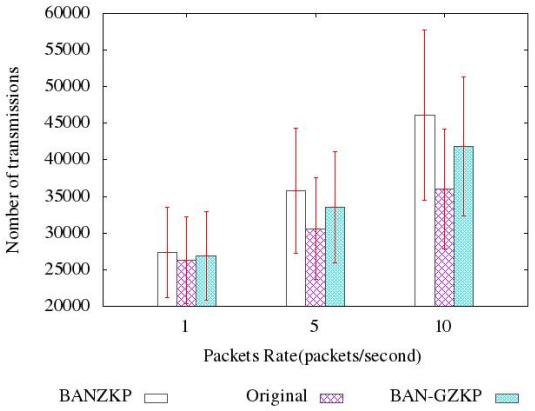

Figure 45: Number of transmissions for CTP in posture 7

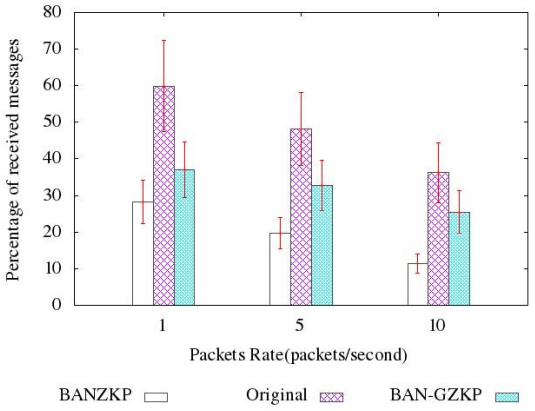

Figure 46: Percentage of received messages for MiniAtt in posture 1

has to ask around its neighbours, who could have the smallest attenuation to the sink. That makes data packets generated by nodes far away from sink need more time and more transmissions to reach the sink than data packets generated by nodes close to the sink. The reception of distant packets extends the average of end-to-end delay and the average of number of transmissions comparing with the original strategy. When plugged with the BANZKP and BAN-GZKP, the additional ZKP message exchange makes it harder for distant packets to reach the sink. As the distant packets occurs fewer percentage of the total packets reception, the average of end-to-end delay and number of transmissions can thus reduce. When comparing BANZKP and BAN-GZKP, in the case of MiniAtt, BAN-GZKP always has better ratio of packets reception and number of transmissions. Additionally it has comparable end-to-end delay in all the postures.

For *FloodToSink* strategy (see Figures from 67

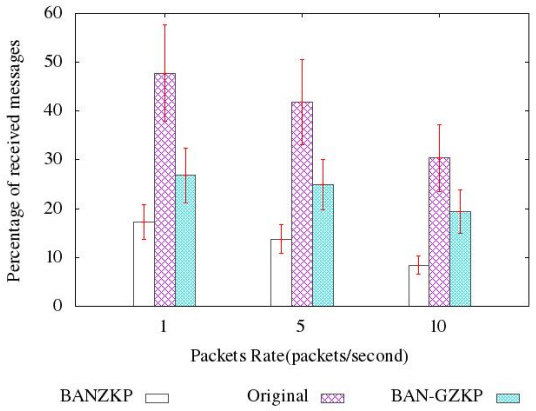

Figure 47: Percentage of received messages for MiniAtt in posture 2

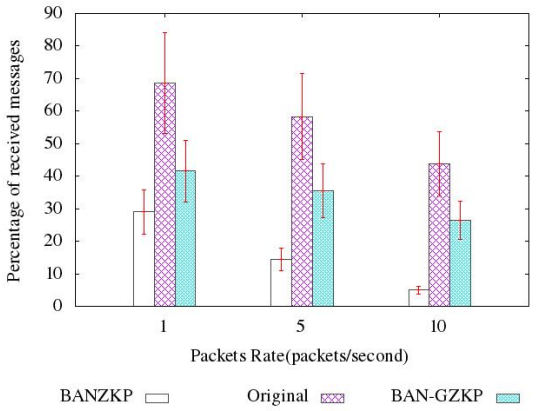

Figure 48: Percentage of received messages for MiniAtt in posture 3

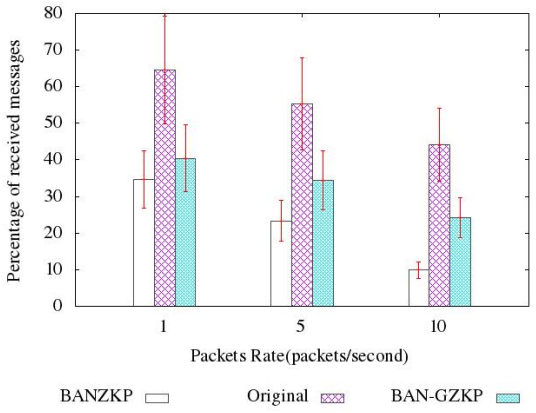

Figure 49: Percentage of received messages for MiniAtt in posture 4

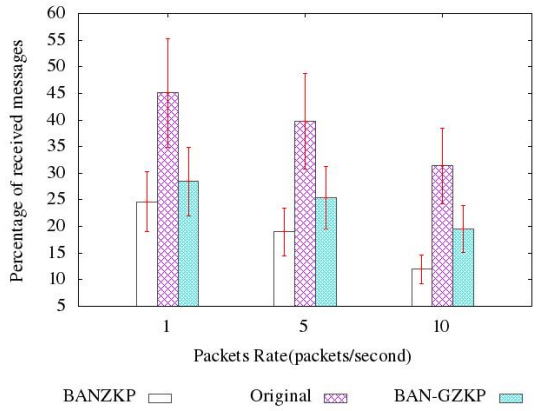

Figure 50: Percentage of received messages for MiniAtt in posture 5

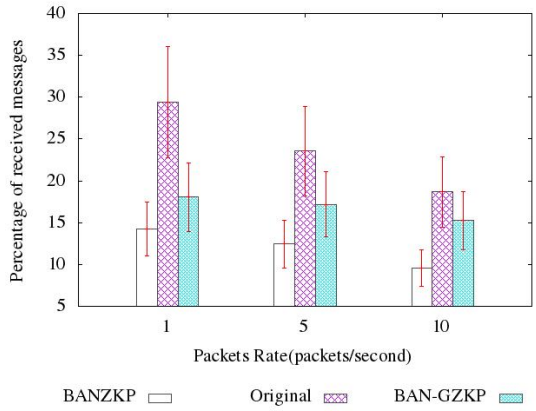

Figure 51: Percentage of received messages for MiniAtt in posture 6

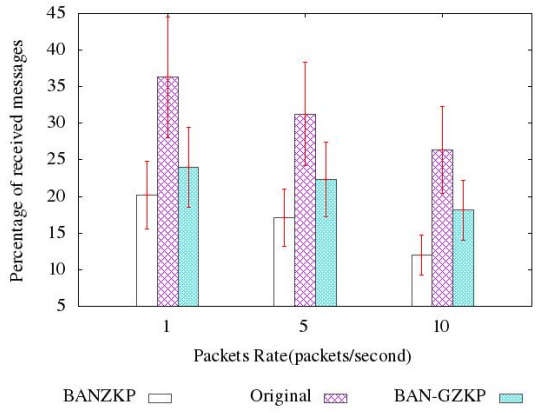

Figure 52: Percentage of received messages for MiniAtt in posture 7

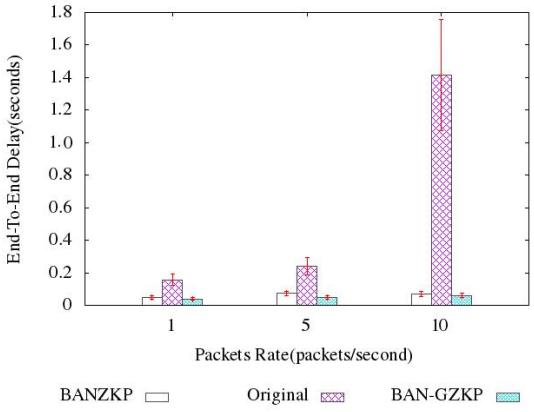

Figure 53: End-To-End Delay for MiniAtt in posture 1

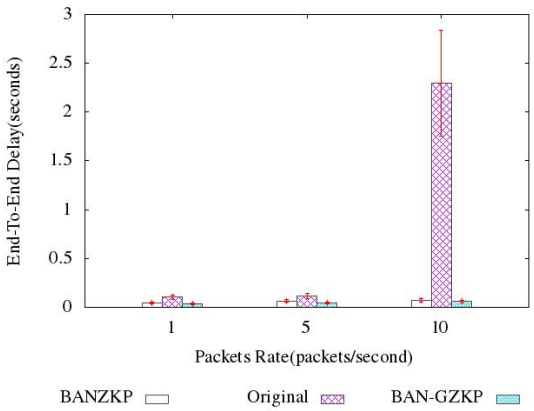

Figure 54: End-To-End Delay for MiniAtt in posture 2

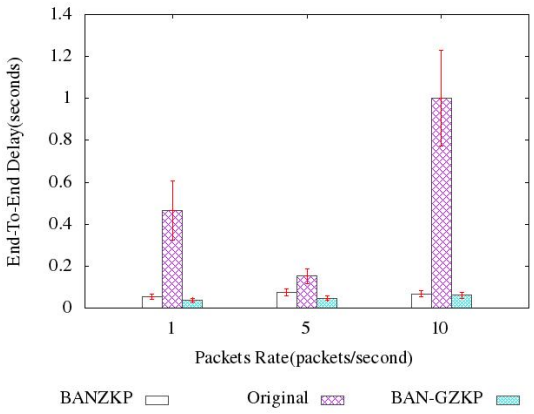

Figure 55: End-To-End Delay for MiniAtt in posture 3

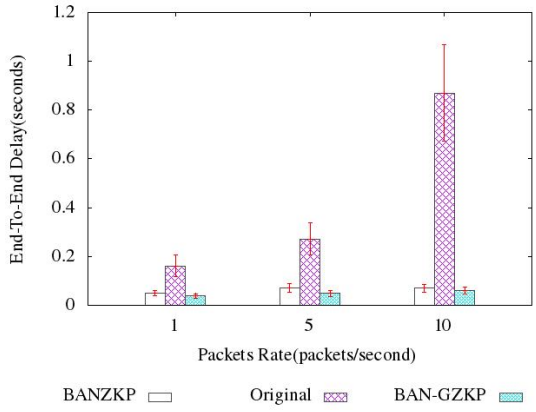

Figure 56: End-To-End Delay for MiniAtt in posture 4

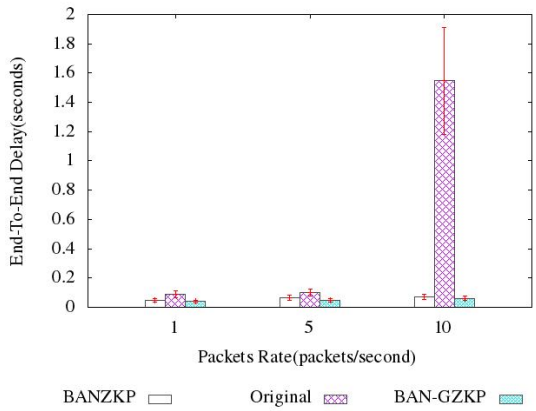

Figure 57: End-To-End Delay for MiniAtt in posture 5

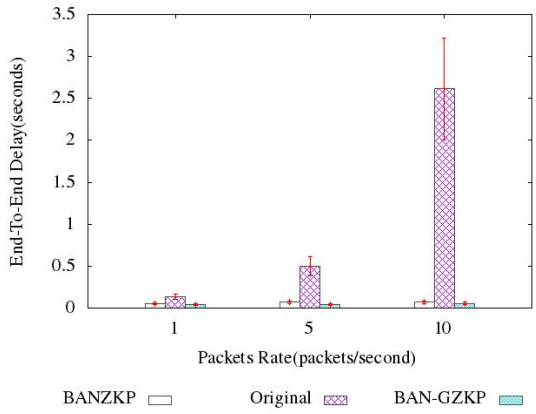

Figure 58: End-To-End Delay for MiniAtt in posture 6

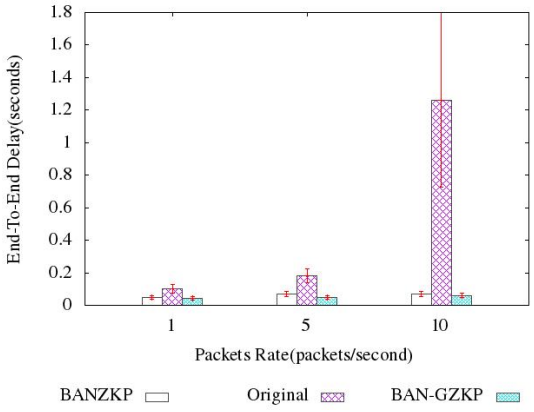

Figure 59: End-To-End Delay for MiniAtt in posture 7

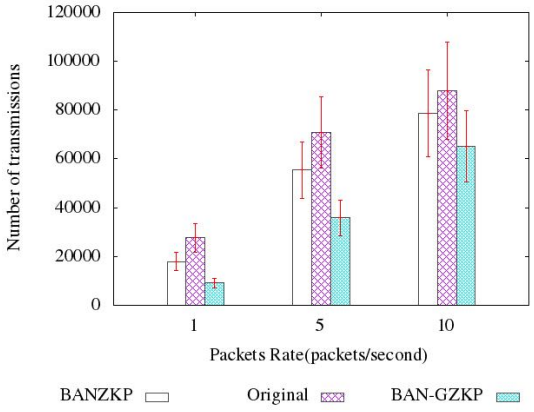

Figure 60: Number of transmissions for MiniAtt in posture 1

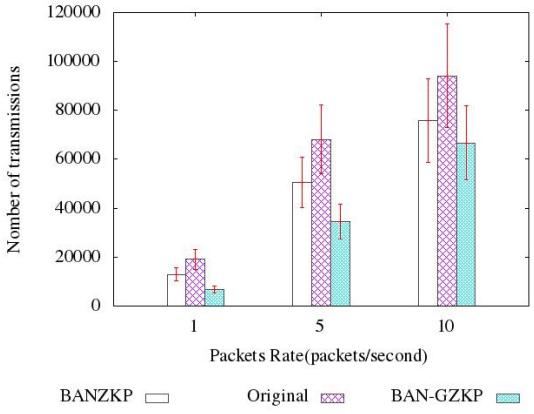

Figure 61: Number of transmissions for MiniAtt in posture 2

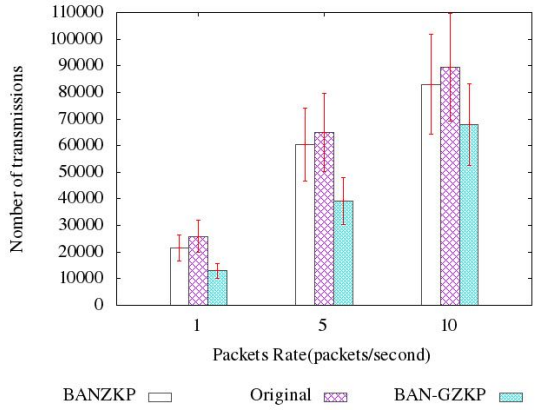

Figure 62: Number of transmissions for MiniAtt in posture 3

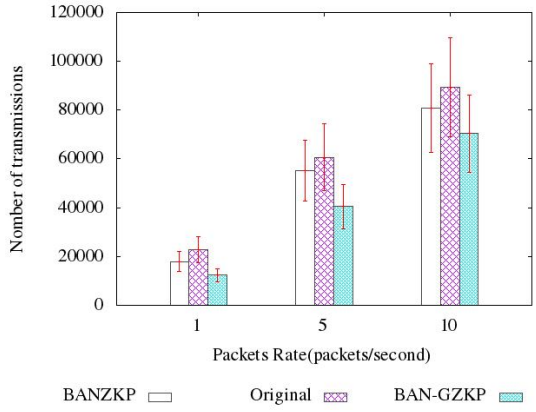

Figure 63: Number of transmissions for MiniAtt in posture 4

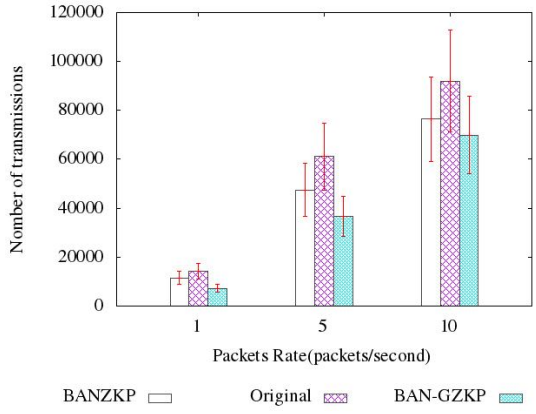

Figure 64: Number of transmissions for MiniAtt in posture 5

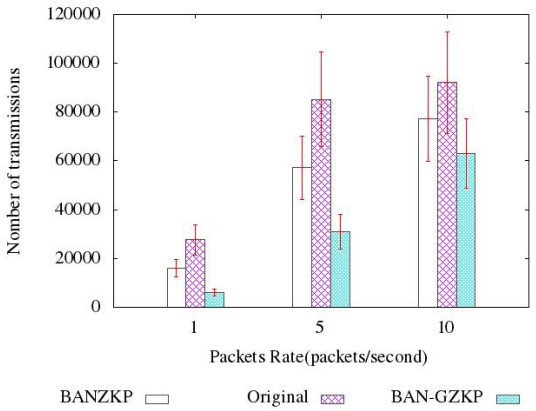

Figure 65: Number of transmissions for MiniAtt in posture 6

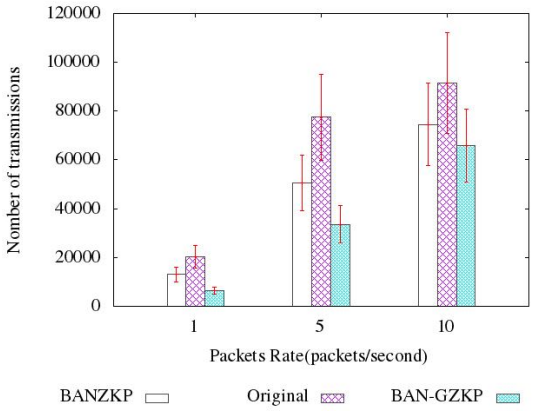

Figure 66: Number of transmissions for MiniAtt in posture 7

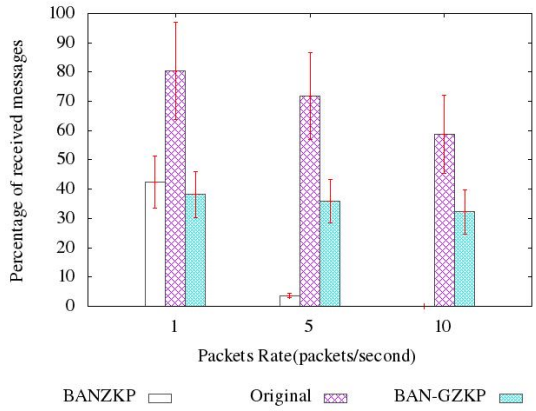

Figure 67: Percentage of received messages for FloodToSink in posture 1

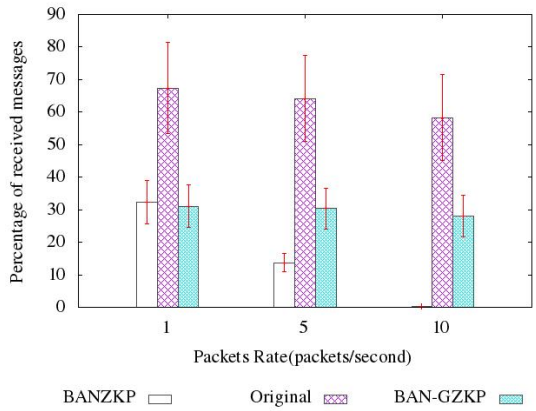

Figure 68: Percentage of received messages for FloodToSink in posture 2

to 87, a example for posture 1 Walking), in general, BAN-GZKP is better than BANZKP, even better than original FloodToSink strategy in terms of number of transmissions. That is because the hop-by-hop BAN-GZKP can limit the flooding transmissions all over the network. In terms of end-to-end delay, BANZKP and the original FloodToSink has varying behaviours in different postures, see Figures 74 and 76: big variance of end-to-end delay, due to its broadcast nature. In terms of ratio of packets reception, original FloodToSink is better when using any ZKP scheme. However the ratio of the packets receptions decreases much faster in the case of BANZKP and original FloodToSink than in BAN-GZKP who is relatively stable. That is because with the increase of the packets generation rate, the number of the packets sent to the network will increase exponentially and lead to the network congestion.

For *TreeBased* strategy (see Figures from 88 to

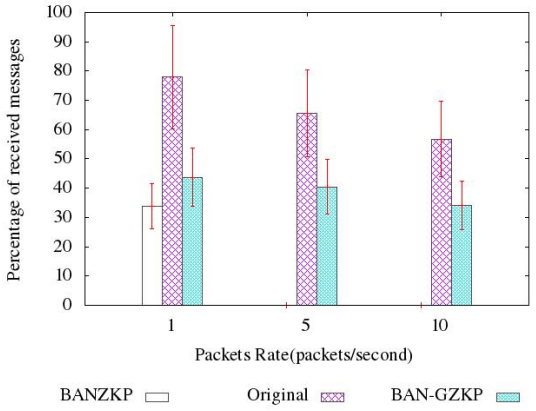

Figure 69: Percentage of received messages for FloodToSink in posture 3

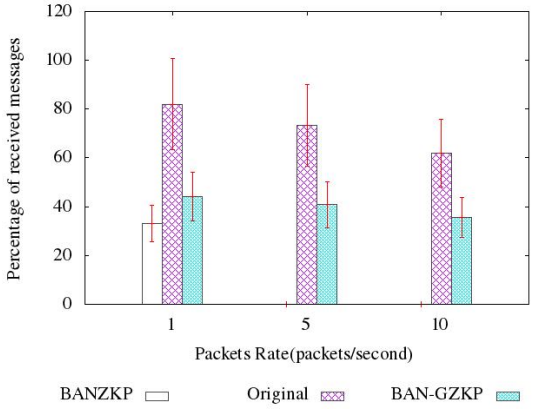

Figure 70: Percentage of received messages for FloodToSink in posture 4

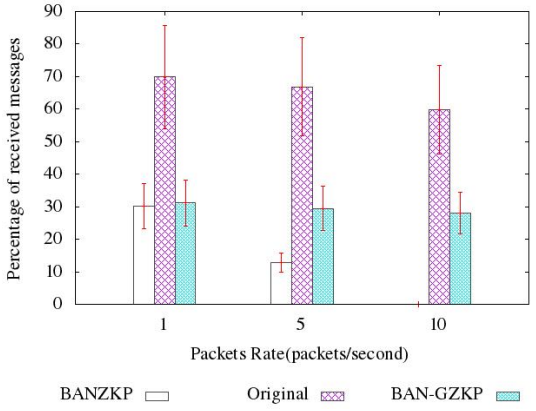

Figure 71: Percentage of received messages for FloodToSink in posture 5

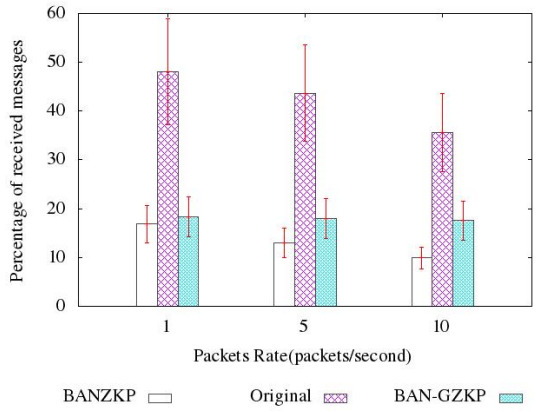

Figure 72: Percentage of received messages for FloodToSink in posture 6

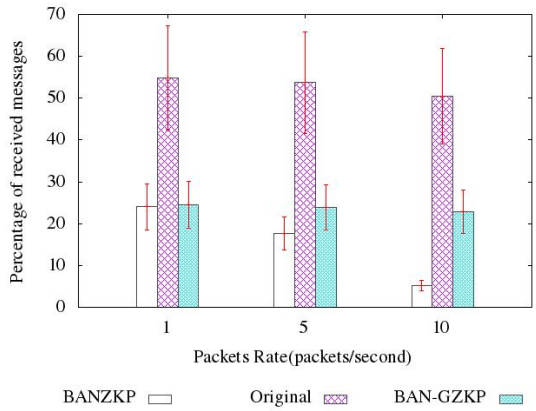

Figure 73: Percentage of received messages for FloodToSink in posture 7

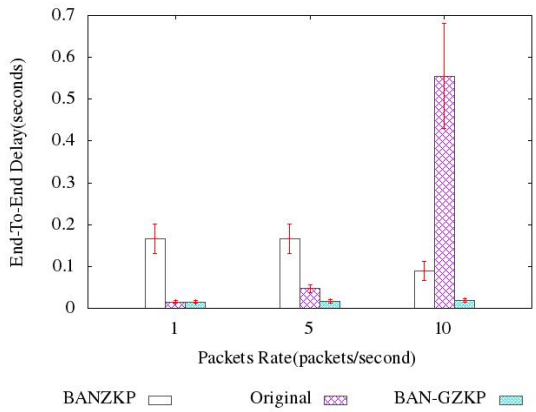

Figure 74: End-To-End Delay for FloodToSink in posture 1

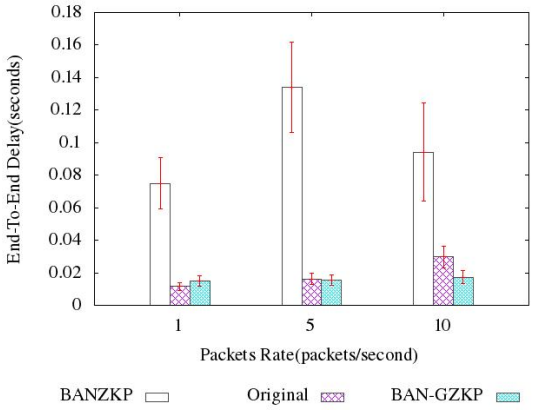

Figure 75: End-To-End Delay for FloodToSink in posture 2

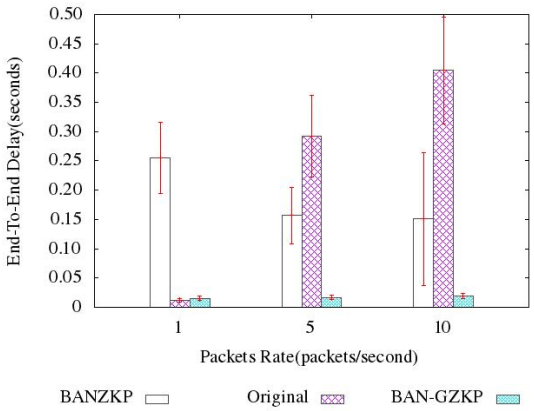

Figure 76: End-To-End Delay for FloodToSink in posture 3

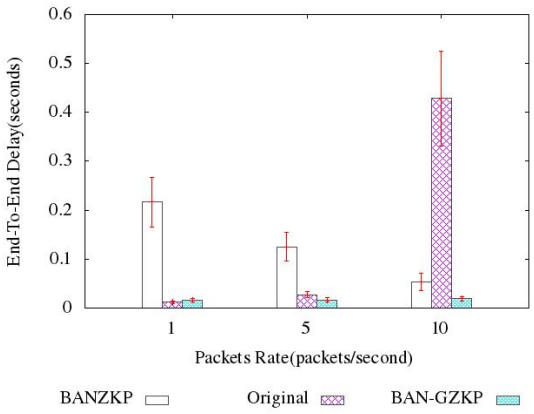

Figure 77: End-To-End Delay for FloodToSink in posture 4

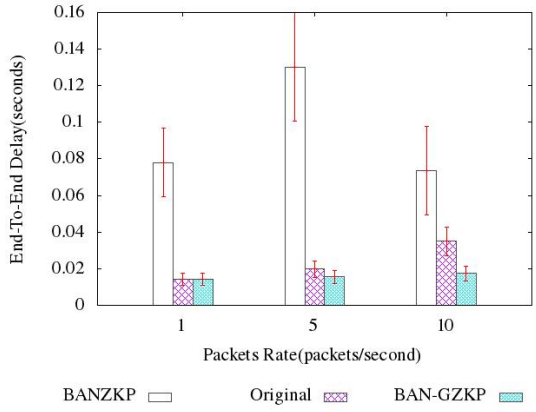

Figure 78: End-To-End Delay for FloodToSink in posture 5

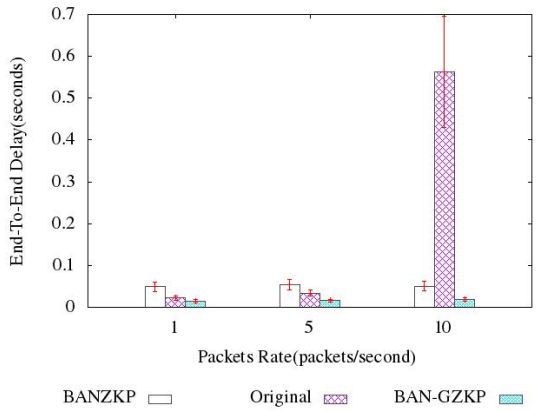

Figure 79: End-To-End Delay for FloodToSink in posture 6

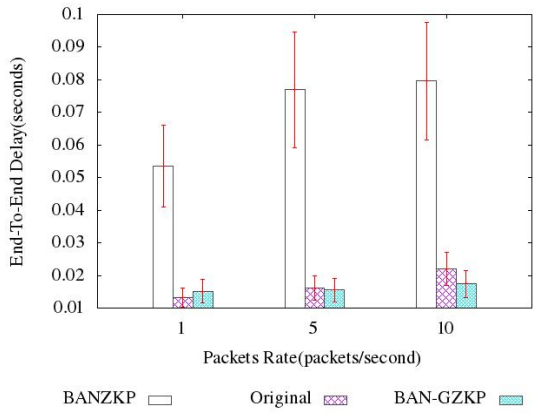

Figure 80: End-To-End Delay for FloodToSink in posture 7

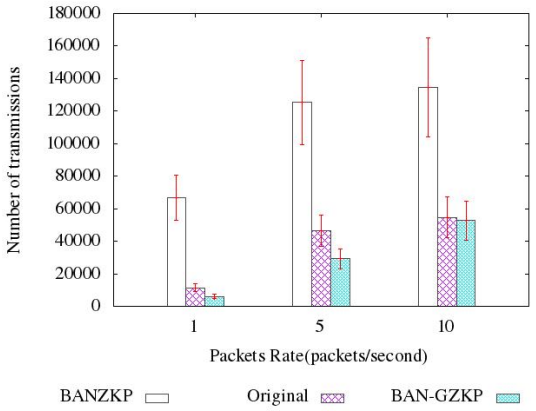

Figure 81: Number of transmissions for FloodToSink in posture 1

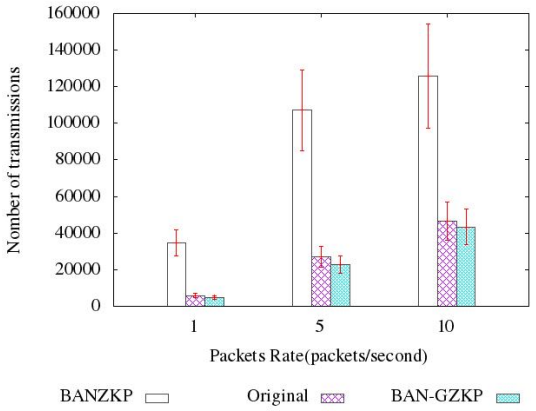

Figure 82: Number of transmissions for FloodToSink in posture 2

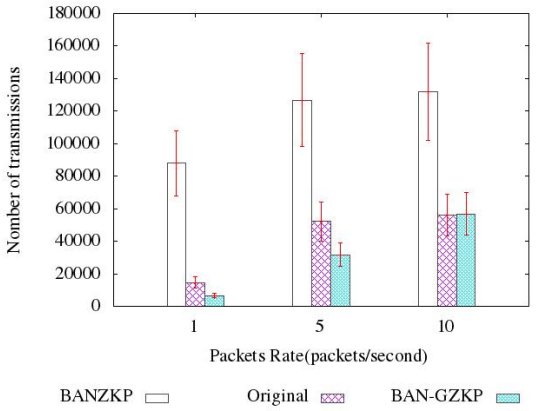

Figure 83: Number of transmissions for FloodToSink in posture 3

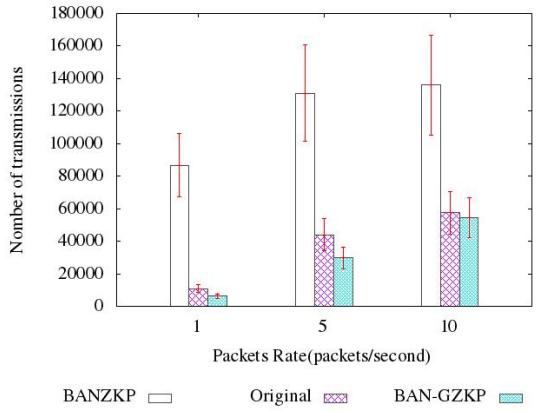

Figure 84: Number of transmissions for FloodToSink in posture 4

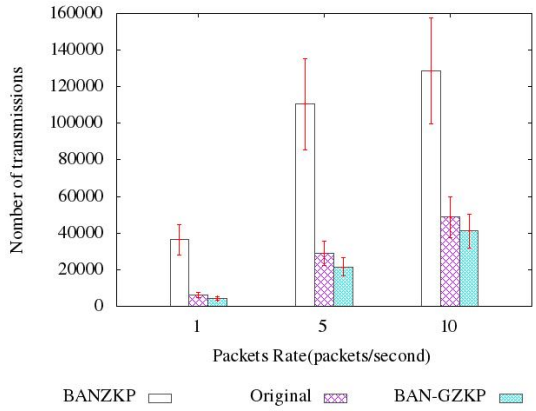

Figure 85: Number of transmissions for FloodToSink in posture 5

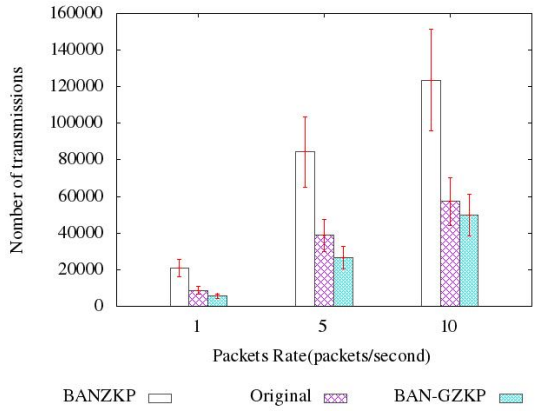

Figure 86: Number of transmissions for FloodToSink in posture 6

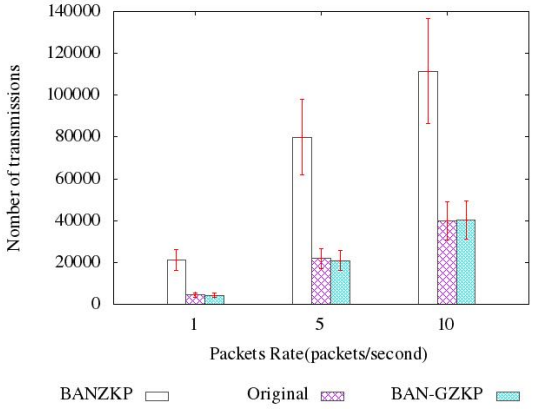

Figure 87: Number of transmissions for FloodToSink in posture 7

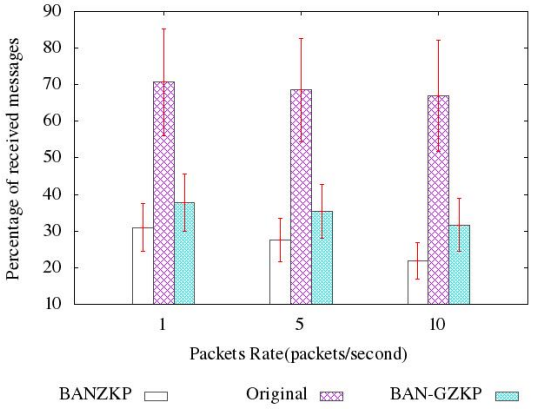

Figure 88: Percentage of received messages for TreeBased in posture 1

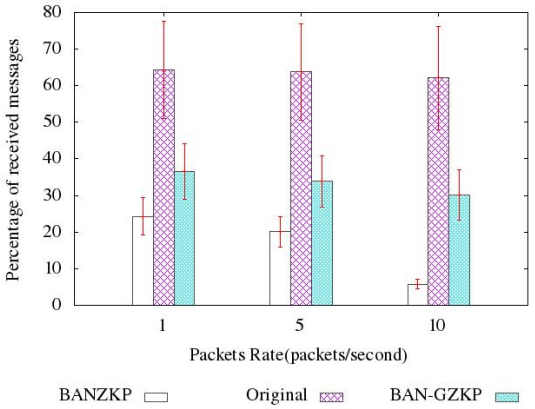

Figure 89: Percentage of received messages for TreeBased in posture 2

108, a example for posture 1 Walking), where packets will be re-sent several times according the links quality. The fast increase of end-to-end delay in case of original TreeBased strategy in postures 6 and 7 (see Figure 100 for example). That because the general networks links quality are not good in posture 6 and 7 [27], the number of the retransmissions in these two postures are important, which lead to important collisions and backoffs with the increase of the packets generation rate. In general, BAN-GZKP has the lower end-to-end delay and number of transmissions in all the postures. In terms of ratio of packets reception, in posture 1, 2, 4 and 7 (see Figure 88 for example), both BAN-GZKP and BANZKP are stable, and BAN-ZKP is better than BANZKP. However in postures 3 and 5 (see Figure 90 for example), BANZKP is better when the packets generation rate is lower than 5 packets per second and 1 packet per second for postures 3 and 5, respectively ; when the packets generation rate is higher than 5 packets per second and 1 packet per second for postures 3 and 5, respectively, the performance of BANZKP decreases fast. And in posture 6, see Figure 93, both BANZKP and BAN-GZKP decrease fast when the packets generation rate is high. That is due to the retransmission mechanism of the TreeBased strategy, which lead to a high network burden. A flawed link not only lead to a decrease of the ratio of packets reception, but also an important number of retransmissions: that consumes the networks resource. If flawed links appear at the edge of the networks, like in postures 1,2 and 7 (see [27]), a hop-by-hop BAN-GZKP will limit the waste of the local retransmissions. But if the flawed links appear close to the sink, like in postures 3, 5 and 6, the BAN-GZKP could waste an important number of transmissions, according to the analyze for strategy APAP and CTP. For the end to end BANZKP, the flawed links do not have an important influence. The defects will be enlarged by the retransmission mechanism of *TreeBased* strategy. The performance of the BAN-GZKP has important variance in defects-enlarged links (by retransmission mechanism) if links defects occur close to the sink.

5. Conclusion

In this paper we proposed a new ZKP-based security scheme specifically designed for WBAN networks. Our scheme, BAN-GZKP uses three ingredients: a novel *random key allocation* which makes it resilient to the replay attack and redundancy information crack, a *hop-by-hop* authentication scheme which makes it resilient to DDoS attacks at sink and a ZKP exchanging optimisation to further reduce the number of transmissions. Our BAN-GZKP improves,

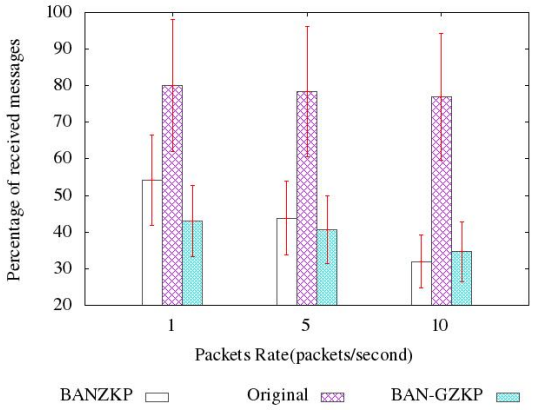

Figure 90: Percentage of received messages for TreeBased in posture 3

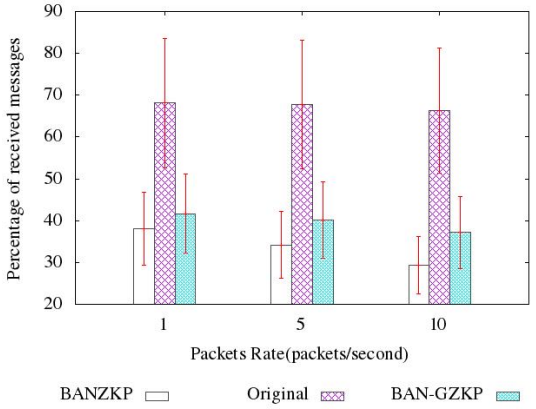

Figure 91: Percentage of received messages for TreeBased in posture 4

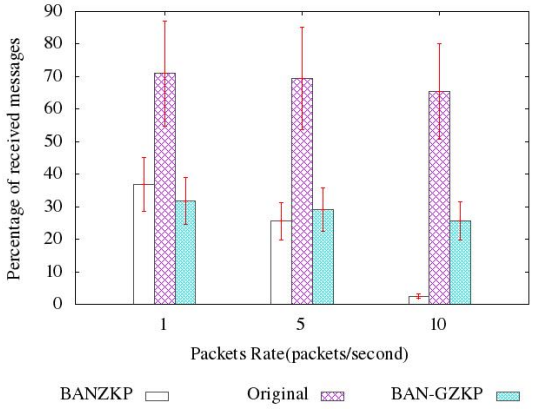

Figure 92: Percentage of received messages for TreeBased in posture 5

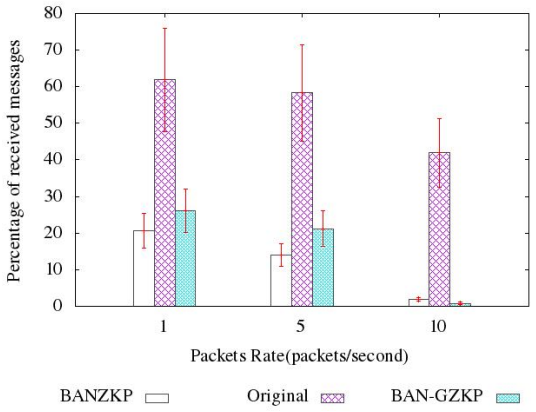

Figure 93: Percentage of received messages for TreeBased in posture 6

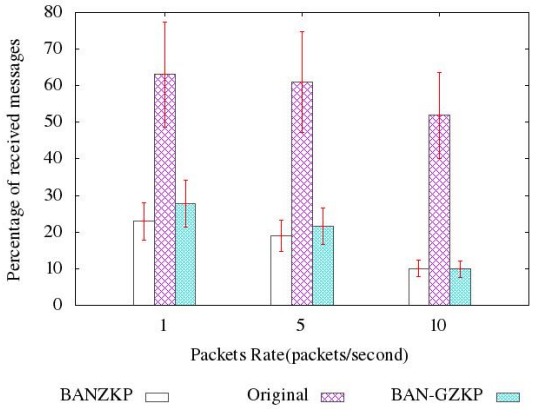

Figure 94: Percentage of received messages for TreeBased in posture 7

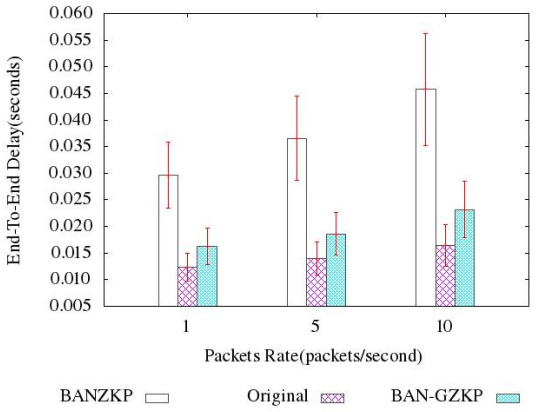

Figure 95: End-To-End Delay for TreeBased in posture 1

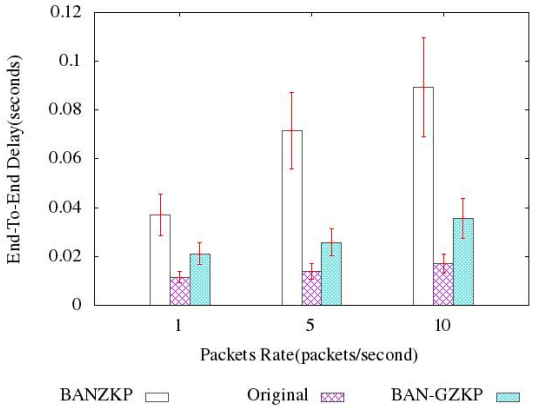

Figure 96: End-To-End Delay for TreeBased in posture 2

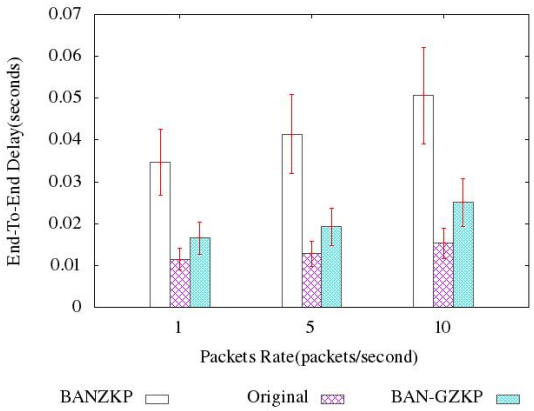

Figure 97: End-To-End Delay for TreeBased in posture 3

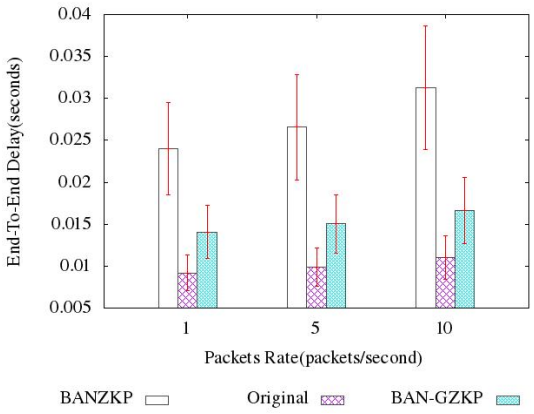

Figure 98: End-To-End Delay for TreeBased in posture 4

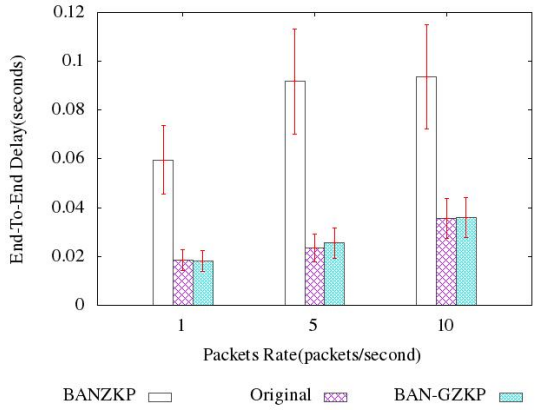

Figure 99: End-To-End Delay for TreeBased in posture 5

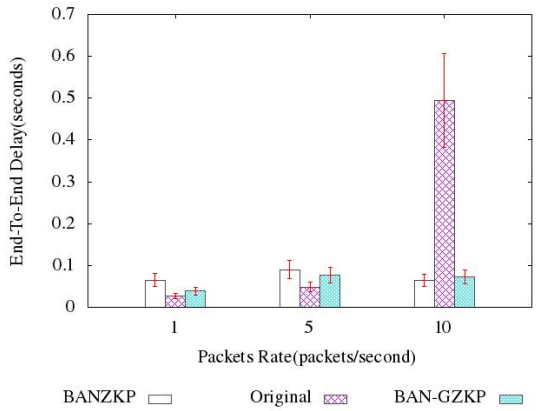

Figure 100: End-To-End Delay for TreeBased in posture 6

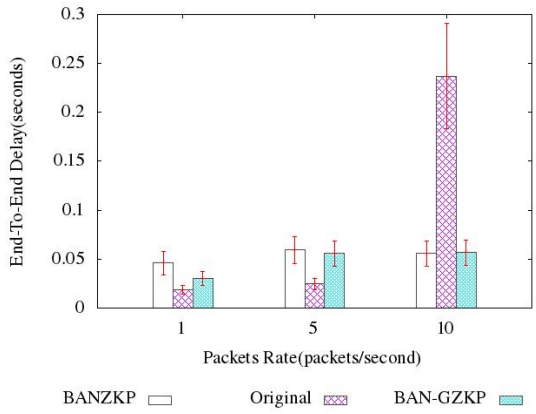

Figure 101: End-To-End Delay for TreeBased in posture 7

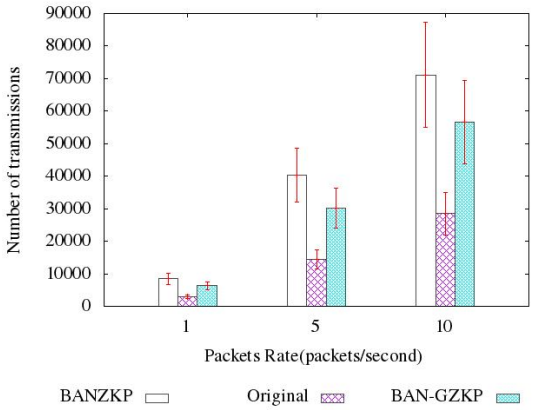

Figure 102: Number of transmissions for TreeBased in posture 1

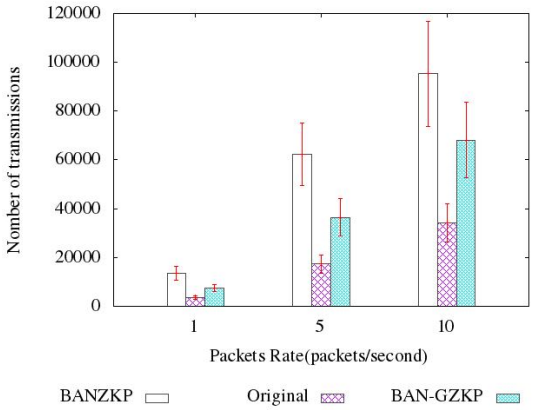

Figure 103: Number of transmissions for TreeBased in posture 2

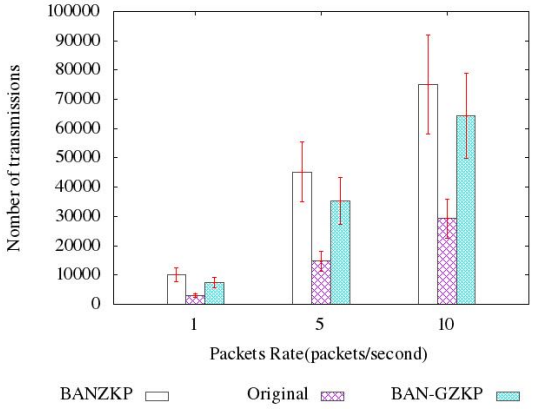

Figure 104: Number of transmissions for TreeBased in posture 3

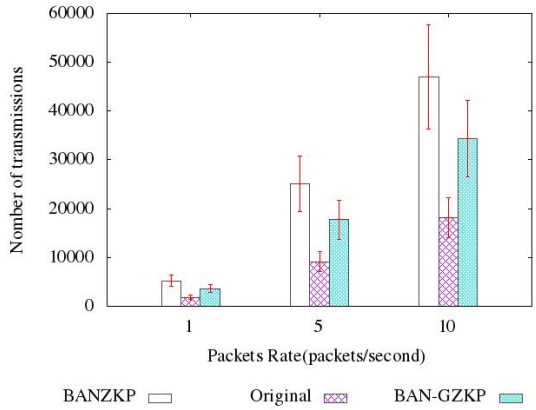

Figure 105: Number of transmissions for TreeBased in posture 4

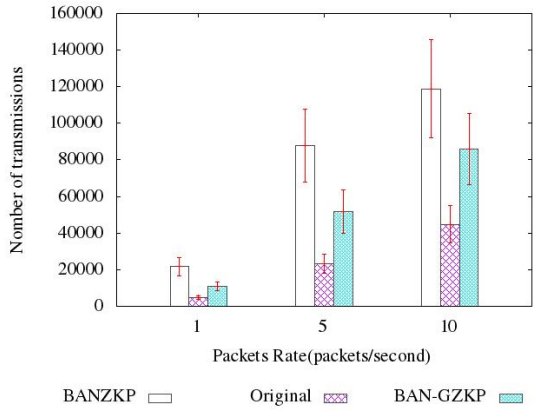

Figure 106: Number of transmissions for TreeBased in posture 5

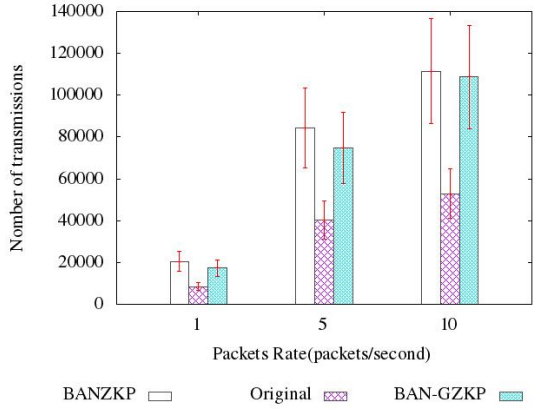

Figure 107: Number of transmissions for TreeBased in posture 6

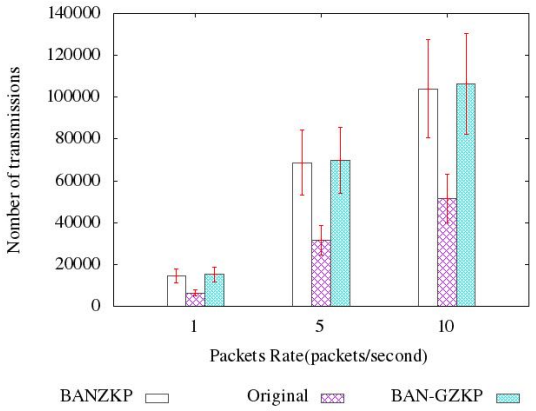

Figure 108: Number of transmissions for TreeBased in posture 7

without any additional cost, the security level of the best ZKP scheme designed so far for WBAN networks. Moreover, when BAN-GZKP is used in order to secure existing convergecast protocols their performances are drastically improved compared to the case when BANZKP is used.

[1] B. Latré, B. Braem, I. Moerman, C. Blondia, P. Demeester, A survey on wireless body area networks, Wireless Networks 17 (1) (2011) 1–18.

[2] T. Hayajneh, G. Almashaqbeh, S. Ullah, A. V. Vasilakos, A survey of wireless technologies coexistence in wban: analysis and open research issues, Wireless Networks 20 (8) (2014) 2165–2199.

[3] J.-i. Naganawa, K. Wangchuk, M. Kim, T. Aoyagi, J.-i. Takada, Simulation-based scenario-specific channel modeling for wban cooperative transmission schemes, IEEE journal of biomedical and health informatics 19 (2015) 559–570.

[4] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, V. Odelu, Secure anonymous mutual authentication for star two-tier wireless body area networks, Elsevier Computer methods and programs in biomedicine 135 (2016) 37–50.

[5] A. A. Omala, K. P. Kibiwott, F. Li, An efficient remote authentication scheme for wireless body area network, Springer Journal of Medical Systems 41 (2) (2017) 25–34.

[6] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, A. Seeam, Pervasive ehealth services a security and privacy risk awareness survey, in: International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), IEEE, 2016, pp. 1–4.

[7] M. Luk, G. Mezzour, A. Perrig, V. Gligor, Minisec: a secure sensor network communication architecture, in: Proceedings of the 6th international conference on Information processing in sensor networks, ACM, 2007, pp. 479–488.

[8] M. Li, S. Yu, J. D. Guttman, W. Lou, K. Ren, Secure ad hoc trust initialization and key management in wireless body area networks, ACM Transactions on sensor Networks (TOSN) 9 (2) (2013) 18.

[9] M. Rushanan, A. D. Rubin, D. F. Kune, C. M. Swanson, Sok: Security and privacy in implantable medical devices and body area networks, in: IEEE Symposium on Security and Privacy (SP), IEEE, 2014, pp. 524–539.

[10] E. Rehman, M. Asad, M. Sher, Ecc and symmetric based hybrid authenticated key agreement implementation and analysis for body sensor networks, Virtual Foundation for Advancement of Science and Technology (VFAST) Transactions on Software Engineering 5 (1) (2015) 1–9.

[11] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, P. Kruus, Tinypk: securing sensor networks with public key technology, in: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, ACM, 2004, pp. 59–64.

[12] G. Sahebi, A. Majd, M. Ebrahimi, J. Plosila, J. Karimpour, H. Tenhunen, Seecc: A secure and efficient elliptic curve cryptosystem for e-health applications, in: International Conference on High Performance Computing & Simulation (HPCS), IEEE, 2016, pp. 492–500.

[13] H. Wang, B. Sheng, C. C. Tan, Q. Li, Public-key based access control in sensornet, Springer Wireless Networks 17 (2011) 1217–1234.

[14] A. Shamir, et al., Identity-based cryptosystems and signature schemes., in: Crypto, Vol. 84, Springer, 1984, pp. 47–53.

[15] Z. Qin, C. Yuan, Y. Wang, H. Xiong, On the security of two identity-based signature schemes based on pairings, Elsevier Information Processing Letters 116 (2016) 416–418.

[16] S. S. Al-Riyami, K. G. Paterson, Certificateless public key cryptography, in: Asiacrypt, Vol. 2894, Springer, 2003, pp. 452–473.

[17] J. Liu, Z. Zhang, X. Chen, K. S. Kwak, Certificateless remote anonymous authentication schemes for wirelessbody area networks, IEEE Transactions on Parallel and Distributed Systems 25 (2014) 332–342.

[18] M. Ramakrishnan, Switch pattern encryption based wban security in an iot environment, Indian Journal of Science and Technology 8 (34).

[19] R. V. Sampangi, S. Dey, S. R. Urs, S. Sampalli, Iamkeys: independent and adaptive management of keys for security in wireless body area networks, in: International Conference on Computer Science and Information Technology, Springer, 2012, pp. 482–494.

[20] T. Choudhary, M. S. Manikandan, Robust photoplethysmographic (ppg) based biometric authentication for wireless body area networks and m-health applications, in: Twenty Second National Conference on Communication (NCC), IEEE, 2016, pp. 1–6.

[21] S. Peter, B. Pratap Reddy, F. Momtaz, T. Givargis, Design of secure ecg-based biometric authentication in body area sensor networks, Multidisciplinary Digital Publishing Institute, Sensors 16 (2016) 570–591.

[22] C. Chaudet, M. Potop-Butucaru, N. Khernane, Banzkp: a secure authentication scheme using zero knowledge proof for wbans, in: The 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, IEEE, 2016, pp. 1–7.

[23] L. Ma, Y. Ge, Y. Zhu, Tinyzkp: a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks, Springer Wireless personal communications 77 (2014) 1077–1090.

[24] G. Bu, M. Potop-Butucaru, Ban-gzkp: Optimal zero knowledge proof based scheme for wireless body area net-

works, in: Mobile Ad Hoc and Sensor Systems (MASS), 2017 IEEE 14th International Conference on, IEEE, 2017, pp. 55–63.

[25] D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on information theory 29 (2) (1983) 198–208.

[26] W. Badreddine, N. Khernane, M. Potop-Butucaru, C. Chaudet, Convergecast in wireless body area networks, Elsevier Ad Hoc Networks 66 (2017) 40–51.

[27] G. Bu, M. Potop-Butucaru, Total order reliable convergecast in wban, in: Proceedings of the 18th International Conference on Distributed Computing and Networking, no. 26, ACM, 2017.

[28] U. Colesanti, S. Santini, The collection tree protocol for the castalia wireless sensor networks simulator, Tech. Rep. 729, Department of Computer Science, ETH Zurich (Jun. 2011).

[29] W. Badreddine, C. Chaudet, F. Petruzzi, M. Potop-Butucaru, Broadcast strategies in wireless body area networks, in: Proceedings of the 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, ACM, 2015, pp. 83–90.

[30] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. Haneveld, T. E. Parker, O. W. Visser, H. S. Lichte, S. Valentin, Simulating wireless and mobile networks in omnet++ the mixim vision, in: Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops, no. 71, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[31] J. Y. Khan, M. R. Yuce, Wireless body area network (WBAN) for medical applications, InTech, 2010, Ch. 31, pp. 591–628.