A secure mechanism design-based and game theoretical model for MANETs

Abderrezak Rachedi, Abderrahim Benslimane, Hadi Otrok, Noman Mohammad, Mourad Debbabi

A Secure Mechanism Design-Based and Game Theoretical Model for MANETs

A. Rachedi and A. Benslimane
LIA/CERI, University of Avignon, Agroparc
BP 1228, 84911 Avignon, France
{abderrezak.rachedi, abderrahim.benslimane}@univ-avignon.fr

H. Otrok, N. Mohammed and M. Debbabi
CIISE, Concordia University,
Montréal, Québec, Canada, H3G 1M8
{h_otrok, no_moham, debbabi}@ciise.concordia.ca

***Abstract*—To avoid the single point of failure for the certificate authority (CA) in MANET, a decentralized solution is proposed where nodes are grouped into different clusters. Each cluster should contain at least two confident nodes. One is known as CA and the another as register authority RA. The Dynamic Demilitarized Zone (DDMZ) is proposed as a solution for protecting the CA node against potential attacks. It is formed from one or more RA node. The problems of such a model are: (1) Clusters with one confident node, CA, cannot be created and thus clusters' sizes are increased which negatively affect clusters' services and stability. (2) Clusters with high density of RA can cause channel collision at the CA. (3) Clusters' lifetime are reduced since RA monitors are always launched (i.e., resource consumption). In this paper, we propose a model based on mechanism design that will allow clusters with single trusted node (CA) to be created. Our mechanism will motivate nodes that do not belong to the confident community to participate by giving them incentives in the form of trust, which can be used for cluster's services. To achieve this goal, a RA selection algorithm is proposed that selects nodes based on a predefined selection criteria function and location (i.e., using directional antenna). Such a model is known as *moderate*. Based on the security risk, more RA nodes must be added to formalize a *robust* DDMZ. Here, we consider the tradeoff between security and resource consumption by formulating the problem as a nonzero-sum noncooperative game between the CA and attacker. Finally, empirical results are provided to support our solutions.**

***Index Terms*—MANET security, mechanism design, certificate authority and clustering.**

I. Introduction

In wired/wireless infrastructure networks, a trusted third party, known as Certification Authority (CA), is needed to certify users' digital certificate that contains users' public key and identity. It is needed to provide a secure communication among users and ensure some security requirements, such as; authentication, confidentiality and integrity of transited data. In classical Public Key Infrastructure (PKI) [9], a Registration Authority (RA) is used to collect and analyze users' requests before forwarding them to a CA to certify, issue and renew user's digital certificate. In Mobile Ad hoc Networks (MANETs), a decentralized certificate authority approach [6], [10], [23] is proposed, due to MANET characteristics, as a solution to avoid single point of failure, MANET attacks and consider nodes' mobility. To handle these requirements, a distributed clustering algorithm is proposed in [22] to cluster nodes based on a set of trusted nodes that belong to a confident community. A head cluster is selected among trusted nodes to play the role of CA. To overcome a single point of failure attack against CA, a set of one-hop nodes, RA, are selected from the set of trusted nodes to form a *Dynamic Demilitarized Zone* ($DDMZ$). The role of these nodes, besides registration authority, is to protect the CA by filtering CA's incoming requests and monitoring the behavior of nodes in the cluster. The approach is suitable once the confident community size is large enough to grant at least two trusted nodes per cluster (i.e., one CA and another RA).

The first limitation of the approach given in [22] is its inability to form clusters with single trusted node and to form the DDMZ from non-confident community. This will decrease the number of clusters and increase clusters' size which affect clusters' services and MANET stability. The second limitation is clusters' lifetime since all selected RA nodes are required to run their monitor and consume resources. Moreover, a high density $DDMZ$ can increase the probability of channel collision at CA. Finally, $DDMZ$ formation is a limitation since RA nodes are selected ignoring CA coverage area. This violates the role of $DDMZ$ since it allows an adversary to launch attacks against CA from RA's uncovered zones.

To overcome these limitations, the $DDMZ$ must be built based on nodes from non-confident community. To build the $DDMZ$ that can cover the CA coverage area, nodes must be cooperative and selected by the CA based on specific selection criteria where some of the parameters of the selection-criteria are considered as private information. The limitations of such a proposition are: (1) Nodes might behave *selfishly* in order not to be selected as RA and consume resources. This will be done by revealing a fake selection-criteria information. To solve such a problem, incentives must be given to nodes to motivate them to participate and serve as RA. The problem that arises here is: How to design the incentives to motivate nodes to participate and reveal their truthful information to build the $DDMZ$? (2) To form the $DDMZ$ that can cover the CA coverage area, node's location is required, which can be used maliciously. To solve such a problem, directional antenna is used to divide the CA coverage area into different sectors in which the RA nodes are selected. Such a model is called as *moderate* since few RA nodes are selected to filter the traffic of CA. The question that we address here is: When to add more RA nodes to form a *robust* $DDMZ$ taking into consideration security and resource consumption? We answer this question by formulating a nonzero-sum non-cooperative game between the CA and attacker where the attacker identity is unknown. Bayesian game theory is used to solve such a game where the CA's threshold value to step to robust $DDMZ$ is computed.

In this paper, we design a unified model that is able to:

- Motivate nodes from non-confident community to serve as RA and build a moderate $DDMZ$.
- Prevent nodes from revealing fake information by designing incentives based on Vickrey, Clarke and Groves (VCG) mechanism where truth telling is the dominant strategy among all nodes.
- Increase the CA protection through the design of moderate $DDMZ$ formation condition that can select RA nodes based on their location.
- Increase the clusters' lifetime by selecting the RA nodes based on a specific selection-criteria function.
- Increase the number of clusters and reduce the cluster's size. This will help to efficiently serve the nodes of the cluster and effect network stability. Moreover, it increases the probability of detecting the misbehaving nodes.
- Run the robust DDMZ mode according to the security needs.

The rest of the paper is organized as follows. In Section II, we discuss the related work on certification authority in MANET and application of mechanism design to networks. In Section III, we provide the problem statement. In Section IV, MANET clustering and CA selection algorithm is given. The moderate $DDMZ$ model is given in Section V where the RA election model, selection criteria function, mechanism model and RA election algorithm are illustrated followed by an example. Section VII presents empirical results. Finally, Section VIII concludes the paper.

II. Related work

This section reviews related work on the distribution of the certificate authority in MANET. Moreover, mechanism design and game theory applications to networks are given.

A. Certification Authority in MANET

In [5], the authors proposed a system based on the distribution of the certification authority among specific nodes by using the threshold cryptography scheme [24] with several threshold levels to offer nodes flexibility in selecting an appropriate security level for a given application. With this approach the fault tolerant and hierarchical key management services are ensured. Unfortunately, the approaches based on threshold cryptography have some drawbacks: Firstly, the n nodes must be initialized by a trusted authority which is responsible for introducing the partial secret of CA role. On the other hand, an external administration is necessary to configure the system and establish the architecture. Secondly, the number k must be a trade-off between availability and robustness, it must be frequently updated. Thirdly, the system overloads the network since the node must send at least k requests instead of sending only one request to obtain a certificate or revocation (i.e., $k-1$ messages are needed).

A few work tried to introduce the fully CA distribution without using the threshold cryptography. We quote the Hubaux et al.'s [6] approach and Satizabal et al.'s [23] system. In these systems, each user is able to generate a certificate for other users. Certificates are stored and distributed by the users themselves. In this system, each user maintains a local certificate repository. When two users want to check the public keys of each other, they merge their local certificate repositories to find appropriate certificate chains. The drawback of this approach is the assumption that trust is transitive and the system becomes more vulnerable to malicious nodes.

Several work introduce the cluster concept for security in MANETs particularly for the CA distribution. Dong et al. [10] and Bechler et al. [4] propose the distribution of the CA service by using threshold cryptography and introduce the cluster structure. The cluster concept is adopted to provide the CA service and proactive secret shared update protocol. In Bechler et al.'s [4] approach, the certification of any guest node must possess a certain number (W) of warranty certificates from warrantor nodes. Then, it must request at least (k) certificates from different cluster heads (CHs), whose association gives the network certificate. Unfortunately, this approach is not realistic because the warrantor nodes do not have any information about the new node to be guaranteed. To overcome this problem, the authors of [22] proposed a distributed architecture which divides the network into clusters and distributes the CA in each cluster to secure the network. They defined a new trust model and new concept of Dynamic Demilitarized Zone (DDMZ) to secure the CA node in each cluster against a single point failure and to monitor the nodes in the cluster.

B. Mechanism Design Application

Mechanism design is a sub-field of microeconomics and game theory [15]. It uses game theory tools to achieve a desired goal. The main difference between game theory and mechanism design is that the former is used to study what could happen when independent players act selfishly, whereas mechanism design allows us to define the game in such a way that the outcome of the game, known as the Social Choice Function (SCF), will be played by independent players according to the rules set by the mechanism designer. Mechanism design has been used in computer science by Nisan and Ronen [19] for solving least cost path and task scheduling problems using algorithmic mechanism design. Distributed mechanism design based on VCG is first introduced in [11] to compute the lowest cost routes for all source-destination pairs and payments for transit nodes on all the routes. It is a direct extension of Border Gateway Protocol (BGP), which causes modest increases in routing table size and convergence time.

Currently in MANET, mechanism design is mainly used for routing purposes. In [2], the authors present a truthful adhoc-VCG mechanism to find the most cost-efficient route in the presence of selfish nodes. In [8], the authors provide an incentive compatible auction scheme to enable packet forwarding service in MANET using VCG. A continuous auction process runs to determine who should obtain how much of the bandwidth and at what price. Incentives are in the form of monetary rewards. On the other hand, mechanism design is recently used for intrusion detection in MANET [21]. The authors propose a distributed election mechanism that selects the most cost efficient node to play the role of leader IDS in a cluster. To motivate nodes to behave normally during the election process, the authors design incentives, based on VCG, in the form of reputation where intrusion detection service is offered to nodes according to their reputation. To catch misbehaving leader after election, a catch an punish model is proposed. As an extension for their work, the authors proposed in [17] a distributed leader-IDS election mechanism that can elect the most cost efficient leaders without running any clustering algorithm.

C. Game Theory Application

Game theory [18] has been successfully applied to many disciplines including economics, political science, and computer science. Game theory usually considers a multi-player decision problem where multiple players with different objectives can compete and interact with each other. Game theory classifies games into two categorizes: Non-cooperative and cooperative. Non-cooperative games are games with two or more players that are competing with each other. On the other hand, cooperative games are games with multi-players cooperating with each other in order to achieve the greatest possible total benefits. To predict the optimal strategy used by intruders to attack a network, the authors of [20] model a non-cooperative game-theoretic model to analyze the interaction between intruders and the IDS in a wired infrastructure network. They solve the problem using a zero-sum non-cooperative game with complete information about the intruder.

In complete information game, the type, strategy spaces, and payoff functions of both players are known. In [1], the authors aim at demonstrating the suitability of game theory for development of various decision, analysis, and control algorithms in intrusion detection. They address some of the fundamental network security tradeoffs, and give illustrative examples in different platforms. They propose two different schemes based on game theoretic techniques and consider a generic model of distributed IDSs equipped with a network of sensors. Bayesian Nash is used in [14] to analyze the interaction between the intruder and defender in static and dynamic scenarios. The authors provide a hybrid detection approach.

These existing studies clearly show that game theory and mechanism design are strong candidates for providing the much-needed mathematical framework for analyzing the interaction between CA and intruders and motivate the nodes to reveal truthfully their selection criteria function. To the best of our knowledge, our work is among the first efforts on securing the CA. We use mechanism design to motivate the nodes to participate on being selected as RA to form the $DDMZ$. A nonzero-sum noncooperative game based on Bayesian Nash equilibrium is used to model the interaction between the CA and intruder, taking into consideration that the precise identity of the intruder is typically unknown. The solution of such a game guides the CA to add more RA nodes according to the game derived threshold.

III. Problem Statement

To protect the CA node, a set of trusted ($T_m = 1$) nodes (one-hop) are selected to play the role of RA and form the *Dynamic Demilitarized Zone ($DDMZ$)* [22]. This is done by filtering the traffic of CA searching for attacks. Moreover, the role of these nodes is to monitor the behavior of other nodes in the cluster. The problems facing this model are: First, the cluster formation requires at least two trusted nodes which prevents clusters with one trusted node to be created. This will lead nodes to join other clusters which increases the number of nodes in the cluster and negatively affect the cluster's services (i.e., routing, intrusion detection, key distribution and certification). Second, all trusted nodes are required to monitor and play the role of RA to ensure security robustness which causes nodes to consume a lot of resources and decrease the cluster's lifetime. Additionally, the more is the RA, the more is the probability of channel collision at CA. Third, it is not granted that the CA coverage area is always monitored by the RA nodes. This is because the $DDMZ$ formation condition did not consider the CA coverage area which can be violated by an attacker.

Solving these problems will start by proposing a solution for cluster formation condition where clusters can be created using one trusted node which is selected as CA. This proposition faces the following challenges: First, nodes that will be selected to play the role of RA, to form $DDMZ$, are no more belonging to the confident community which can lead nodes to behave *selfishly*. We define *selfish node* as an economically rational node whose objective is to maximize its benefits (payoffs). Second, RA selection will be based on specific criteria such as energy level, trust level, mobility and connectivity degree. Some of these information are considered as private where nodes can reveal fake information in order not to be selected and preserve their resources. Incentives must be given in the form of trust in order to motivate nodes to reveal their private information. The question arises here is: How to design the incentive in such a way where truth telling is the dominant strategy for all nodes? Third, to increase the cluster's lifetime and to avoid channel collision, a specific number of nodes must be selected to form the $DDMZ$. Moreover, these nodes should be able to monitor the CA coverage area by filtering all the CA traffic. The question that we address is: What is the minimum number of RA nodes needed to achieve this goal? Such a model is known as moderate since few nodes are selected to form the $DDMZ$. Finally, to increase the security of the $DDMZ$, RA nodes have to be added to the sector where the probability of attacks is high. Such a model is known as robust $DDMZ$. The question that arises here is:

When to step from moderate to robust $DDMZ$? What is the security threshold needed to step to robust $DDMZ$?

In this paper, we propose a new $DDMZ$ formation condition where RA nodes will be selected by the CA based on their selection-criteria function which is defined in terms of nodes' private information. Here, we assume that the CA is equipped with an antenna that can work as directional or omni-directional. RA election algorithm is designed where the directional antenna is used to create the $DDMZ$ by selecting a set of RA nodes that meet the selection criteria. This will increase the robustness of $DDMZ$. On the other hand, omni-directional antenna is used to overhear the RA nodes and monitor their behavior. Moreover, we propose a model based on VCG mechanism [13] to motivate nodes to reveal truthfully their private information. Payments are issued in the form of reputation (trust) to motivate nodes to say the truth. Finally, we model a nonzero-sum noncooperative game to find the security threshold needed to step from moderate to robust $DDMZ$. These propositions will help to increase the cluster's security and lifetime and reduce channel collision at the CA.

IV. MANET Clustering and CA Election Algorithm

In this section, we devise a clustering algorithm that clusters MANET and elects a CA in each cluster. To ensure the security, it is assumed that set of the nodes belong to a confident community. For clusters with more than one trusted node, the CA is selected among these nodes based on node's stability which increases cluster's lifetime. Furthermore, the clustering algorithm ensures the authentication and integrity of the transited data during the election process.

Each trusted node sends two successive *hello* message in order to calculate the Relative Mobility (RM), after that, it announces itself as CA with a certain cluster's size (k-hop). When a trusted node receives a beacon, from one of its neighbors, it executes clustering algorithm 1 to change its status from cluster-head (CA) to cluster-member. The decision to change the status from CA to cluster-member depends on two main parameters: Security and stability. A CA is considered as more stable than others if it has a low relative mobility. Any trusted node with relative mobility more than a specific threshold is considered as unstable and thus will not be considered during the CA selection. The nodes situated between two adjacent clusters can become gateway (GW) [22]. Algorithm 1 is executed by each node that belongs to confident community. where, $Packet-Authentication-Integrity-checking()$ is the function which consists to check the integrity and the authentication of the election packet. $HopCount$ indicates the hop number of the election packet.RM_i is the relative mobility of node i and DN_i is the degree of the neighbors nodes of the node i.

Once the CA node is elected per cluster, it starts to transmit cluster's beacon in order to inform the cluster's member nodes about its availability. The cluster's nodes that are not receiving any beacon from a CA for a predefined period of time is considered as unavailable.

Algorithm 1: Clustering Algorithm ($SDCA_{V2}$)

When node j receives an election packet from node i;
begin
  Packet-Authentication-Integrity-checking();
  if *($HopCount >= k$)* **then** $\mathbf{No-Competition}$; $\mathbf{Goto(end)}$;
  else if *($RM_i < RM_j$) OR (($RM_i == RM_j$) AND ($DN_j < DN_i$))* **then**
    Accept node i as CA;
  else if *($RM_j < RM_i$) OR ($DN_j > DN_i$)* **then**
    node j remains as CA candidate;
  else if *($RM_i == RM_j$) AND ($DN_j == DN_i$)* **then**
    apply Lowest-ID;
end

V. A Moderate $DDMZ$ Model

In this section, we present our RA election mechanism for truthfully electing the RA nodes that will serve as $DDMZ$ and belong to non-confident community. In Subsection V-A, we describe the RA election model followed by the selection criteria function F for electing RA nodes is given in Subsection V-B. Subsection V-C formulates our mechanism model using with the payment function followed by an example.

A. RA Election Model

Once the CA node of each cluster is selected, it elects a set of RA nodes that belongs to non-confident community with a certain trust-level. The RA nodes are located at one-hop from the CA node. The role of RA nodes is to protect CA node against attack from unknown nodes such as Denial of Service (DoS). Any packet destined to CA node must be analyzed and filtered by RA nodes. To achieve this goal, a moderate $DDMZ$ should be created by selecting the best RA nodes based on nodes' selection criteria function and according to nodes location. This will increase the performance of $DDMZ$ since the CA coverage area is protected by RA nodes. Selecting RA nodes according to their location requires a secure localization algorithm [7]. To avoid running such algorithm, directional antenna is used by the CA where the CA's zone is divided into 6 sectors [12]. The sectors are numbered from 1 to 6 starting with zone 1 heading east as shown in figure 1. Dividing the CA zone to 6 sectors with 250 m omni transmission range leads to 450 m of directional transmission range [12]. With such type of antenna, the CA node can allocate the location of one-hop nodes. This proposition allows us to prolong cluster's lifetime by electing the minimum number of RA nodes that covers the 6 sectors. With 250 m of omni transmission range, each RA node can cover its own sector and the left and right sectors. This means that 3 RA nodes are required to form a moderate $DDMZ$ where RA nodes are selected from **disjoint sectors**. This means that RA nodes cannot be selected from the same sector or from two consecutive sectors. For example, if a CA

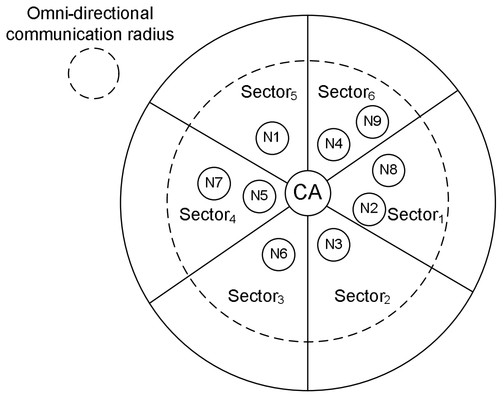

Fig. 1. Cluster of 10 nodes divided into 6 Sectors

chooses node N_3 then nodes from sectors 1, 2 or 3 cannot be selected. Thus, DDMZ can be formulated by selecting nodes from sectors $\{1, 3, 5\}$ or $\{2, 4, 6\}$. The selection between both combination depends on the selection criteria function $F()$ given in subsection V-B. This formation condition will increase the monitoring coverage area for the cluster and thus the DDMZ is efficiently able to protect the CA node from attacks originated from different directions. The objective of maximizing the selection-criteria function (F) of $DDMZ$ can be expressed by the following Social Choice Function (SCF):

$$SCF = S(C) = \max \sum_{i \in N} F_i \tag{1}$$

This means that the summation of F given in Subsection V-B of the selected RA nodes has to be maximum overall the set of possible combination. Clearly, to maximize the summation, the nodes need to reveal their truthful function F. In the next subsection, we design a mechanism design based incentive model for encouraging each node in revealing its true function value.

B. Selection Criteria Function (F)

The selection criteria function has the following parameters:

Trust Level/Metric (Z_1): This metric determines the confident level of nodes which is evaluated by the monitoring mechanism. Each node has a reputation generated by the monitoring mechanisms according to its contribution in the network like forwarding ratio or others network' services.

Stability Metric (Z_2): RA node's stability is based on the relative mobility according to the CA node (it is the private information of a node). The mobility metric is based on the power level (received signal strength) detected at receiving node *RxPr*, it is indicative of the distance between the transmitting and receiving node pairs. The ratio of *RxPr* between two successive packets transmissions gives a good knowledge about the relative mobility between two neighboring nodes. The relative mobility metric at node Y with respect to X is defined by $RM_y^{rel}(x)$ [3].

$$RM_Y^{\mathrm{rel}}(X) = 10 \log_{10} \frac{RxPr_{X \to Y}^{\mathrm{new}}}{RxPr_{X \to Y}^{\mathrm{old}}} \tag{2}$$

Residual Energy Metric (Z_3): This metric determines the residual energy level of the nodes. This is also a private information of a node.

Connectivity Degree (Z_4): It is the number of links a node is connected with. In other word, connectivity degree is the number of one hop neighbors of a node. A node having greater connect degree means that it can cover more nodes for monitoring in the cluster.

Based on the above four parameters, our selection criteria function F is defined as follows:

$$F = \sum_{i=1}^{4} W_i Z_i \tag{3}$$

where W_i is the weight of each parameter i. According to the security context, the weight of the trust metric (W_1) must be greater than others metrics. However, the stability (W_2) and the residual energy (W_3) have the same weight, because both metrics have the same importance in the model. When the stability metric is low, the RA node cannot be insured for its role for long time. On the other hand, when the residual energy metric is low, the RA will not be able to do its task for long time. Finally, the connectivity degree metric (W_4) has the lowest weight since it does not impact the security of the cluster. If the connectivity degree is low, then more RA nodes are needed for coving the whole cluster. Therefore, we can establish the relation between metrics' weight as follows: $W_1 > W_2 = W_3 > W_4$ and $\sum_{i=1}^{4} W_i = 1$.

The stability and residual energy are the private information, which needs to be truthful in order to have a truthful calculated function F. We give incentive in terms of reputation so that nodes are motivated to participate and reveal their truthful function $F()$. To achieve this goal, the payment should be designed in such a way truth-telling is the dominant strategy for each node.

C. Mechanism Model

We treat the RA election as a game where the N mobile nodes are the agents/players. Each node plays by revealing its own private information (selection criteria function (F)) which is based on the node's type θ_i. The type θ_i is drawn from each player's available type set Θ_i={*Normal*, *Selfish*}. Each player selects his own strategy/type according to how much the node values the outcome (i.e., The amount of reputation granted). If the player's strategy is normal then the node reveals the true selection criteria function F. We assume that each player i has a utility function [15]:

$$u_i(\theta_i) = p_i - v_i(\theta_i, \mathbf{o}(\theta_i, \theta_{-i})) \tag{4}$$

where,

- θ_{-i} is the type of all the other nodes except i.
- v_i is the valuation of player i of the output $\mathbf{o} \in O$, knowing that O is the set of possible outcomes. In our case, if the node is elected then v_i is the value of the selection criteria function F_i.

- $p_i \in \Re$ is the payment given by the mechanism to the elected node. Payment is given in the form of reputation. Nodes that are not elected receive no payment.

Note that, $u_i(\theta_i)$ is what the player usually seeks to maximize. It reflects the amount of benefits gained by player i if he follows a specific type/strategy θ_i. Players might deviate from revealing the truthful value of the function F if that could lead to a better payoff. Therefore, our mechanism must be strategy-proof where truth-telling is the dominant strategy. To play the game, every node declares its corresponding function F, where each node's reported function value is the input for our mechanism (i.e., input vector). For each input vector, the mechanism calculates its corresponding output $\mathbf{o} = o(\theta_1, \ldots, \theta_n)$ and a payment vector $\mathbf{p} = (p_1, \ldots, p_n)$. Payments are used to motivate players to behave in accordance with the mechanism goals. The goal of our mechanism is to motivate nodes to say the truth and compute the output **o** that is equal to the SCF defined in Equation 1.

Payment Design: Based on the selection criteria function revealed by all the nodes to the mechanism, CA elects a set of nodes according to the requirement to play the role of RA that forms the $DDMZ$. Our mechanism provides payments to the elected RAs for running their monitor and forming a $DDMZ$. The nodes that are not elected will not not receive any payment. The payment is in the form of reputations, which are then used to increase the trust level and allocate the cluster's services. Hence, any node will strive to increase its reputation in order to increase the trust level.

According to VCG [2], the following design of payment is strategy proof where truth-telling is the dominant strategy:

$$p_i = F_i + \sum_{i \in N} v_i(o*) - \sum_{j \in N} v_j(o*) \tag{5}$$

where o^* is the optimal selection of nodes that maximizes the sum of all the agent's declared function value. Here, $\sum_{j \in N} v_j(o*)$ denotes the second maximum summation assuming without node i.

D. RA Election Algorithm

Once the CA node is determined by Algorithm 1, it elects the RA nodes for the cluster. Initially, the CA sends $Start - Election$ message to each sector according to Algorithm 2 using the directional antenna. Then, the CA waits for the reply from the member nodes for a fixed interval of time, T_1. On expiration of T_1, it sends the $Start - Election$ to the next sector. Thus, steps 2 and 3 are repeated for all the 6 sectors. At the end of T_6, the CA accumulates all the values of function F from the member nodes. Then, it determines the RAs according to the equation 1 and calculates the payment according to equation 5. Finally, CA sends a $Payment - confirmation$ message to the elected RAs.

Algorithm 2: Executed by CA node

1. **For** Sector 1 to 6:
2. Sends $Start - Election$ message to its neighbors;
3. Wait for the reply from the member nodes;
4. **End For**
5. Determine the RA nodes for $DDMZ$;
6. Send $Payment - confirmation$ to the RAs;

On the other hand, member nodes wait for the $Start - Election$ message from CA. Once received, it calculates the function value, F and sends it to CA for optimal RA determination. The member nodes then wait for the election results from the CA. Elected RA nodes receive a $Payment - confirmation$ message from the CA and it launches its monitor to perform the role of RA.

Algorithm 3: Executed by Member nodes

1. Receive $Start - Election$ message from CA;
2. Calculate and Send the Function value F to CA node;
3. **If** node receive $Payment - confirmation$ from CA;
4. Play the role of RA;
5. **end If**;

E. Example

To illustrate the RA election scheme, we consider the cluster of Figure 1. Since our model is repeatable, we present the election process at the 10^{th} round. The reputation at the 9^{th} round is given in the first row of Table I.

TABLE I
$DDMZ$ FORMATION EXAMPLE

Nodes	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9
Reputation 9^{th}	100	80	75	60	50	65	110	120	60
Function Value	3	5	9	8	7	6	6	5	3
Reputation 10^{th}	100	80	84	72	58	65	110	120	60

To elect the RA nodes in the 10^{th} round, the CA node sends $Start - Election$ message to all the sectors one after another. Upon receiving the $Start - Election$ message, the member nodes send their function value, F to the CA node according to Algorithm 2 and 3. The corresponding function values are given in the second row of Table I. Then, the CA node elects the RA nodes based on RA selection model (Section V-A). Here, the winners (or elected RAs) are nodes N_3, N_4 and N_5 since the summation of their function value is maximum, which is 20. Moreover, the CA calculates the payments of the elected RAs according to equation 5. For example, the payment for the node N_3 is $P_3 = 5 + (20 - 16) = 9$. This is because if node N_3 did not participate then the winners would have been nodes N_1, N_2 and N_6 and thus the maximum summation would have been 16. Similarly, the payments for the node N_4 is $P_4 = 8 + (20 - 16) = 12$ and N_5 is $P_5 = 7 + (20 - 19) = 8$. Finally, the CA sends a $Payment - confirmation$ message to the elected RA nodes and increases the reputation of the nodes which is shown in the third row of Table I. On receiving the confirmation, the elected nodes launches the monitors to play to role of RA.

F. Cluster Risk Assessment Strategies

In order to allocate a security level to the cluster, the CA must assess the security risk. The cluster security risk is an important parameter that indicates to the CA if the security level needs to be increased or decreased. In this paper, the cluster security risk is called the cluster risk factor (CRF). The assessment of the CRF is complex, because it depends on many uncertain parameters such as :

- The probability of attack against the CA node, which depends on the probability of attacks against the RA nodes. If the attacker wants to launch an attack against the CA, it must first attack the RA nodes (DDMZ).
- The probability that there are attackers in the cluster, which depends on the number of unknown nodes in the cluster. If there are unknown nodes, it means that the trust model does not have enough information about them. Then the potential attacker nodes may belong to this class of unknown nodes.
- The probability to compromise the trusted nodes. The trusted nodes may be captured and the private information may be disclosed.
- The probability to attack the gateway nodes in order to disconnect some clusters from the network.
- Probability of DoS attacks against the $DDMZ$. An attacker can launch jamming attacks against the $DDMZ$ area in order to prevent the RA and CA nodes from communicating. This requires more than one attacker to be able to run such type of attack since RA nodes belong to different sectors.

In order to make the security level in the cluster dynamic and to design a reactive security model, the CA node must assess the possibility of having any of the cluster security risk events. The risk assessment strategies are presented in Figure 2.

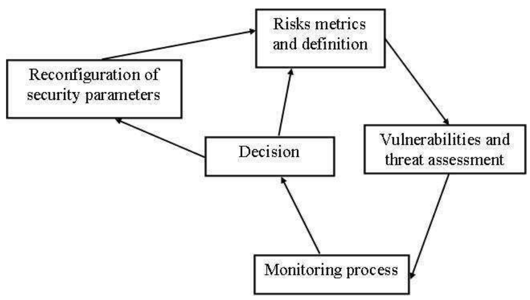

Fig. 2. Cluster Risk Assessment Strategies

The risk metrics and definitions: In order to accurately measure the potential impact of a risk in the cluster, a set of important parameters must be defined and dynamically updated. These parameters must be enough exhaustive to ensure the good working of the cluster.

The vulnerability and threat assessment : At this stage, the configuration of the cluster must be scanned and evaluated. For example, the number of RA nodes, the arrival rate of unknown nodes, the CA area coverage and the nodes density in the cluster. This information is important to assess the vulnerability of the cluster and its effectiveness.

The monitoring process: It allows us to monitor the nodes behavior in order to detect the malicious activities. In each cluster, the set of RA nodes plays the role of the monitor nodes and generates a report for each node belonging to the cluster. For example, the cooperative and malicious nodes activities can be the subject of monitoring.

The decision: At this stage, the decision regarding the reconfiguration of security parameters is made. The decision depends on the results of the monitoring process, the vulnerability and threat assessment stages. This step gives us some information about how to manage the risk, we identify three reactions options: 1) To accept the risk and not to react, 2) To mitigate the risk by increasing the security level, which can effect nodes resources, 3) To interrupt the services and transfer the risk to other nodes which are able to manage the risks. Here, we selected choice two and we propose a solution that consider both security and resource consumption.

Reconfiguration of the security parameters: The reconfiguration depends on the decision stage. The goal of this stage is to mitigate the risk and to avoid the attacks. For example, when the risk is considered high, the number of RA nodes must be increased. In the following section, we derive the security threshold that is needed to reconfigure our $DDMZ$.

VI. A Moderate to Robust Game Model

The RA election model, proposed before, can form a moderate $DDMZ$ since one RA is monitoring and filtering the CA's incoming traffic for almost three sectors. This model can be used whenever the probability of attack is low. It will help to reduce the overall resource consumption of a cluster. Once the probability of attack against the CA is high, the CA should add more RA nodes to the sectors in which an attack has been launched from. The CA is able to allocate the side from which an attack is generated from since CA's incoming traffic must be forwarded from a RA. Therefore, the CA decides that the $DDMZ$ must step into the robust mode in these sectors by adding more RA nodes. A mechanism is needed to decide when to go from moderate mode to robust mode. To formally address this issue, we formulate a game with two players: CA and intruder. The objective of the intruder is to attack the CA node without being filtered by the RA. To achieve this an attacker can either tries to compromise the RA node or to overload it with high density of traffic that can lead the RA to forward some packets to the CA without filtering.

A. The Game Definition

We model the game as nonzero-sum noncooperative game with incomplete information about the players where each player has a private information about his/her preferences. In our case, the CA type is known to all the players while the sender type is selected from the type set $\Theta = \{$*Malicious (M), Normal (N)*$\}$. Knowing that the sender type is a private information. *Bayesian Equilibrium* [25] dictates that sender's

TABLE II
MODERATE TO ROBUST GAME

Strategy	Robust	Moderate
Attack	$\overline{E_r}V - C_a, \quad E_rV - C_r$	$\overline{E_m}V - C_a, \quad E_mV - C_m$
Not-Attack	$0, -C_r$	$0, -C_m$

action depends on his/her type θ. By observing the behavior of the sectors, we can determine the behavior of the sender at time t_k, the CA can calculate the posterior belief evaluation function $\mu_{t_{k+1}}(\theta_i|a_i)$ using the following Bayes' rule:

$$\mu_{t_{k+1}}(\theta_i|a_i) = \frac{\mu_{t_k}(\theta_i)\ P_{t_k}(a_i|\theta_i)}{\sum_{\theta_i \in \Theta} \mu_{t_k}(\theta_i)\ P_{t_k}(a_i|\theta_i)} \quad (6)$$

where $\mu_{t_k}(\theta_i) > 0$ and $P_{t_k}(a_i|\theta_i)$ is the probability that strategy a_i is observed at this stage of the game given the type θ of the node i. It is computed as follows:

$$P_{t_k}(Attack|\theta_i = M) = E_m \times O + F_m(1 - O)$$

$$P_{t_k}(Attack|\theta_i = N) = F_m$$

where O is the observed behavior, which is determined by the CA monitor. F_m is the false rate generated by the CA. E_m is the expected detection rate by a RA (moderate mode).

We define the intruder's pure strategy as $A_i = \{Attack, Not\_Attack\}$. On the other hand, CA strategy is selected from the strategy space $A_{IDS} = \{Robust, Moderate\}$. By solving this game using pure strategy, there is no Nash equilibrium. Thus, mixed strategy is used to solve the game where q is the probability to run in robust mode and p is the probability to attack by the attacker. In Table II, the game is defined where the utility function of the CA by playing the *Robust* strategy while the attacker plays the *Attack* strategy is defined as $E_r\ V - C_r$. It represents the payoff of protecting the CA node, which values V, from being compromised by the attacker, where $E_r\ V >> C_r$. On the other hand, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_r}\ V - C_a$. It is considered as the gain of the attacker for compromising the CA node. Additionally, we define $E_m\ V - C_m$ as the payoff of IDS, if strategy *Moderate* is played while the attacker strategy remains unchanged. Conversely, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_m}\ V - C_a$. Now, if the attacker plays *Not-Attack* strategy and the CA strategy is *Robust* then the losses of the CA is C_r while the attacker gains/losses nothing. Moreover, the payoff of the attacker with the same strategy and CA strategy is *Moderate* is 0 while the losses of the IDS is defined as C_m which is the cost of running the CA in moderate mode. Where,

- $\overline{E_r} = 1 - E_r$, where E_r is the expected detection of an attack in the robust mode.
- E_m is the expected detection in the moderate mode. On the other hand, $\overline{E_m}$ is equal to $1 - E_m$.
- C_r is the cost of running the $DDMZ$ in robust mode. We define the cost as the aggregation of the cost of monitoring by the RAs.
- C_m is the cost of running the $DDMZ$ in moderate mode.
- C_a is the cost of attack by the attacker.
- V is the value of the CA (asset).

B. The Game solution

To solve the game and find the optimal values of p and q, the CA and attacker compute their corresponding utility functions followed by the first derivative of the functions. From Table II, the CA utility function U_{CA} is defined as follows:

$$U_{CA} = [qp(E_r\ V - C_r) + p(1-q)(E_m\ V - C_m) - q(1-p)C_r$$

$$-(1-q)(1-p)C_m]\mu(\theta = M) - [qC_r + (1-q)C_m](1 - \mu(\theta = M))$$

The main objective of the CA is to maximize this utility function by choosing for a fixed p^*, a q^* strategy that maximizes the probability of protection and leads to equilibrium where the following holds:

$$U_{IDS}(p^*, q^*) \geq U_{IDS}(p^*, q)$$

To achieve this goal, the CA will calculate the optimal value of p^* by finding the first derivative with respect to q^* and setting it to zero. This will result to the following: $p^* = \frac{C_r - C_m}{\mu\ V\ (E_r - E_m)}$

The value of p^* is used by the CA to decide whether to add more RAs to the region where an attack came from. The CA computes the belief μ, as in Equation 6, of each RA's region which reflects the sender belief. If the sender type is *malicious* and decided to attack by launching an attack the expected probability to be detected by CA is E_m. Since the attack could be launched iteratively and missed in the coming iterations, the CA will decide to add more RA nodes in the region in which an attack is observed, if the probability of attack is greater than $p^* = \frac{C_r - C_m}{\mu\ V\ (E_r - E_m)}$.

On the other hand, the utility function U_a of the attacker is defined as follows:

$$U_a = qp(\overline{E_r}\ V - C_a) + p(1-q)(\overline{E_m}\ V - C_a)$$

The main objective of the attacker is to maximize this utility function by choosing for a fixed q^*, a p^* that maximizes the probability of compromising the victim node and leads to equilibrium where the following holds:

$$U_a((p^*|\theta = M), q^*) \geq U_a((p|\theta = M), q^*)$$

To maximize the utility function, it is sufficient to set the first derivative with respect to p^* to zero which will be equal to: $q^* = \frac{C_a - \overline{E_m}\ V}{(E_r - E_m)\ V}$.

From the solution of the game, the attacker best strategy is to attack once the probability of running the $DDMZ$ in robust mode is less than $q^* = \frac{C_a - \overline{E_m}\ V}{(E_r - E_m)\ V}$. To achieve this, the attacker will observe the behavior of the CA at time t_k to

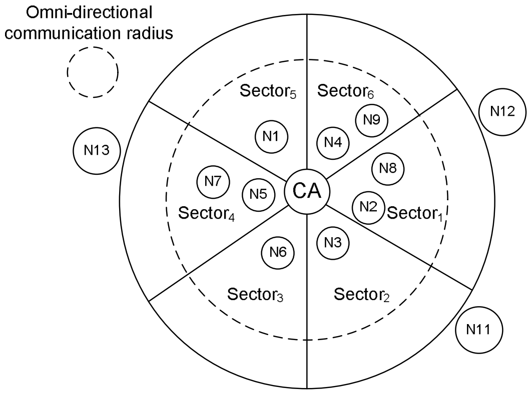

Fig. 3. 3 external nodes with N_{11} is attacking CA

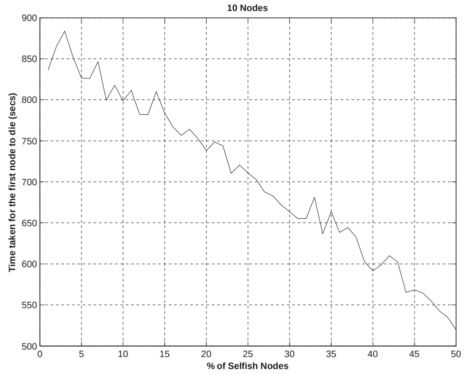

Fig. 4. Impact of selfish node on the lifetime of Network

determine whether to attack or not at time t_{k+1} by comparing its estimated observation with the derived threshold.

C. Example

After the RA election is completed, the $DDMZ$ is in moderate mode where each RA is responsible for monitoring and filtering its coverage area which is more than one sector. To demonstrate how more RA nodes are added according to the security needs, we show the interaction between CA and 3 external nodes. As an example, we select node N_3 as the RA node where an intruder is targeting to attack the CA through it. Figure 3, describes an attack scenario where an attack could be directed to CA node either from node N_{11}, N_{12} or N_{13}. Hence, the CA will use the belief function of Equation 6 to calculate the belief of each RA's region (more than one sector) using the prior observed actions. For example, we assume that the CA's belief regarding each RA's region which reflects external node's belief is $\mu = \{\mu_{11} = 0.7, \mu_{12} = 0.2, \mu_{13} = 0.1\}$. According to RA region's belief, the CA computes the threshold that determines the behavior of the external nodes (i.e., attack or not). If the probability of attack is greater than the computed threshold then the CA should add more RA nodes to the region in which an attack came from. For example, if the threshold of attack by node N_{11} is 0.18, assuming that $C_r - C_m$ = 10, $V_{CA} = 100$ and $E_r - E_m$ = 0.83, then the CA node will add more RA nodes to the region where N_3 is allocated. This is because the value of the CA, with respect to the cluster, is much more than the cost of running the $DDMZ$ in robust mode. Hence, launching the $DDMZ$ in robust mode by adding more RA nodes to the region in which an attack came from is affected by the ratio of monitoring cost to the value of the CA node (i.e, security of the cluster).

VII. Simulation Results

In this section, we evaluate and compare the performance of the new proposed secure clustering algorithm ($SDCA_{V2}$) with the previous model $SDCA_{V1}$ [22]. We have implemented our clustering algorithm as described previously. We use the Network Simulator (NS-2) [16] with CMU wireless extensions to simulate our algorithm. Simulation scenarios were generated with parameters listed in table III.

TABLE III
SIMULATION PARAMETERS

Parameter	Value in our simulation
Number of nodes (N)	50
Network size (mxn)	$670x670m2$
Mobility	[0-20 m/sec]
Transmission Range	50 m - 250 m
Pause time	3.0 s
Simulation time	200 s

At first, we motivate our work showing the impact of selfish nodes on the network. As mentioned before, nodes can behave selfishly before the election. A node shows selfishness before election by refusing to serve as RA. This selfishness has a serious impact on resource consumption of the normal nodes. Figure 4 depicts the impact of selfish nodes on the life of normal nodes. The result indicates that normal nodes will carry out more the duty of RA and die faster whenever the number of selfish nodes increase. Thus, the presence of selfish node effect the lifetime of the entire network.

After we illustrated the impact of selfishness on the lifetime of normal nodes, we need to show the performance of our model on both: number of clusters and DDMZ formation. In Figure 5.(a), we show the average number of CA nodes that can create clusters. The figure shows that as the transmission range increases the number of clusters decreases for both models. Due to the new cluster formation conditions, the number of CA nodes of our model $SDCA_{V2}$ is greater than the previous one $SDCA_{V1}$. In $SDCA_{V1}$, clusters are formulated by at least two trusted nodes, where as in $SDCA_{V2}$, cluster formation needs one trusted node. Hence, we can conclude that the new model ($SDCA_{V2}$) is more flexible than the previous one with respect to cluster's formation. Thus, nodes' CA service will be enhanced and probability of detecting the misbehaving nodes can be increased since nodes will be distributed over more number of CAs.

Now, we need to show that the selection criteria function F and the directional antenna selection are needed to form a moderate DDMZ. First, we analyze the distribution of the RAs

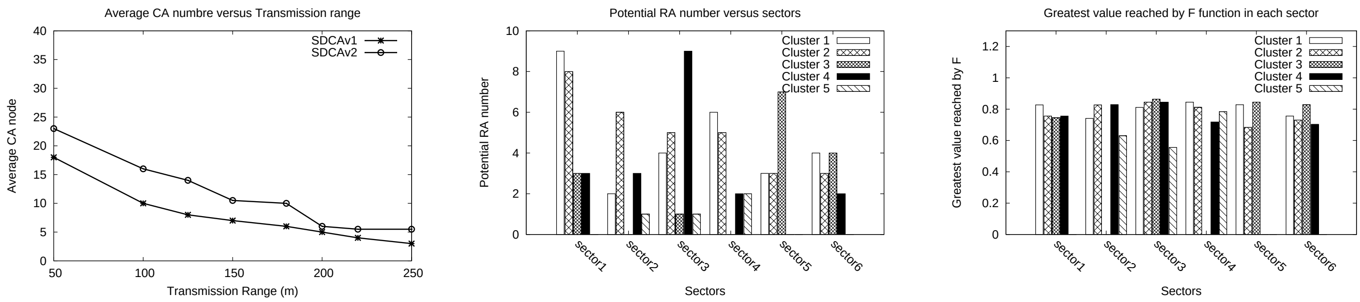

Fig. 5. (a) The average CA node versus transmission range (b) The potential RA node number/sector (transmission range=250m) (c) The maximum value reached by F()/sector with transmission range=250m and $w_1 = 0.5$, $w_2 = w_3 = 0.2$ and $w_4 = 0.1$

in each cluster according to our proposed directional antenna selection model. Our clustering algorithm divides 50 nodes over 5 clusters when the transmission range is $250m$. Figure 5.(b) illustrates the number of potential RA nodes in each cluster's sector. We notice that cluster 5 does not have enough RAs to form a moderate DDMZ. Selecting the nodes based on the selection criteria can still be valid and nodes will be motivated to reveal their function F but selected RA nodes cannot cover the CA coverage area. On the other hand, the other clusters have sufficient RAs to form a moderate DDMZ. As an example, cluster 1 has RAs in all sectors. Thus, it can form a moderate DDMZ by selecting RAs from sectors 1, 3, 5.

Finally, we show how the value of function $F()$ is used to select RAs. Figure 5.(c) shows the maximum value reached by the function $F()$ in each clusters' sector. This information is useful for the CA in order to select the RA nodes since the function $F()$ determines the ability of the RA nodes to form a moderate DDMZ. We notice that in cluster 3, sector 3 has the maximum value of $F()$ among all the sectors. However, $F()$ value is null in sectors 2 and 4. Hence, the CA will choose RA from sector 1, 3, 5. Thus, the CA nodes select the RAs not only based on the function $F()$, but also based on the location (the sectors in which it belongs to) of the RA nodes in order to form a moderate DDMZ.

To simulate our moderate to robust model, we assume that the CA is able to detect attacks that are not filtered by the RA node. The output of the CA ranges between 0 and 1. If the computed output is less than 0.8 then it is classified as a normal behavior, otherwise it is abnormal (attack). Figure 6.a shows the behavior of an external node (node N_{11} in the previous example) for two different attack scenarios for 40 consecutive rounds. To determine the type of the sender (N_{11}), the posterior belief function is calculated using Equation 6 with prior belief $\mu_0 = 0.5$, $F_m = 0.1$ and $E_m = 0.83$. Figure 6.b shows the posterior belief of the leader for these two attack scenarios. The belief for the first attack scenario converges to 1 faster than the second attack scenario. This is because in the first scenario the attacker starts to attack earlier compared to the second scenario. Once the belief reaches 1, it does not go down even if the attacker is not attacking since the type already been identified. After calculating the belief, the CA computes the attack threshold. The CA adds more RA nodes in the sector in which that attack came from. Figure 6.c illustrates the cumulative energy consumption by robust $DDMZ$ for the two attack scenarios (i.e., having more RA nodes added). We assume that the robust $DDMZ$ mode consumes 5 joules of energy for one round. Thus, if the robust $DDMZ$ mode is always monitoring it consumes $40 \times 5 = 200J$ for the 40 rounds. On the other hand, in our model the $DDMZ$ consumes $145J$ and $100J$ for the two attack scenarios respectively. This will prolong the $DDMZ$ lifetime. Thus, the robust $DDMZ$ mode is launched according to the security needs.

VIII. CONCLUSION

The Dynamic Demilitarized Zone (DDMZ) is previously proposed as a solution for protecting the CA node against potential attacks. It is formed from one or more RA nodes where the CA and RA nodes belong to the confident community. Clusters with one confident node, CA, cannot be created and thus clusters sizes are increased which negatively affect clusters services and stability. Moreover, clusters with high density of RA can cause channel collision at the CA. Additionally, clusters lifetime are reduced since RA monitors are always launched and thus more resources are consumed. Thus, we proposed a model based on mechanism design that allow clusters with single trusted node (CA) to be created. The mechanism is able to motivate nodes that does not belong to the confident community to participate by giving them incentives in the form of trust, which can be used for clusters services. Moreover, a RA selection algorithm is proposed that selects nodes based on a predefined selection criteria function (F) and nodes location. This will lead to a moderate DDMZ that is able to preserve the security of CA and prolong the lifetime of clusters. Once the probability of attacks is high, more RA nodes have to be selected to form a robust $DDMZ$. To achieve this goal, we formulated the problem as a nonzero-sum noncooperative game between the CA and attacker. The solution of the game guided both the CA and attacker to their optimal strategy against each other. Thus, the optimal threshold to step from moderate to robust $DDMZ$ is derived. Simulation results indicate that our model lead to more number of clusters and moderate DDMZ can be created based on both:

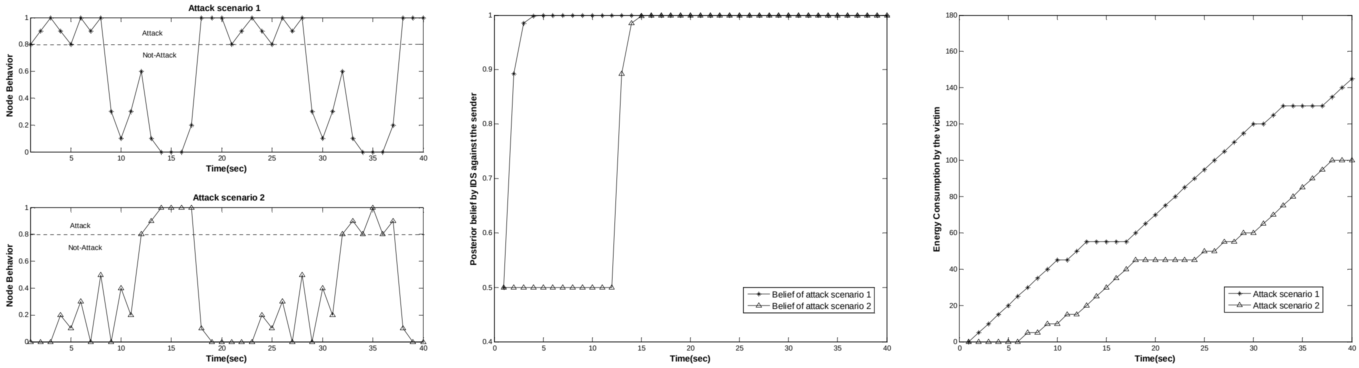

Fig. 6. (a) Attack scenarios (b) Posterior Belief (c) Energy consumption by the victim

selection criteria function (F) and directional antenna selection model. Moreover, the robust $DDMZ$ is called according to the security risks, which prolongs cluster's lifetime.

REFERENCES

[1] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. In *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC)*, 2004.

[2] L. Anderegg and S. Eidenbenz. Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. *Proceedings of the ACM MobiCom'03, San Diego, California, 2003*.

[3] P. Basu, N. Khan, and T. Little. A mobility based metric for clustering in mobile ad hoc networks. In *In Proceedings of Distributed Computing Systems Workshop*, pages 43–51, 2001.

[4] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf. A cluster-based security architecture for ad hoc networks. In *Proceeding of IEEE INFOCOM'2004*, pages 2393– 2403.

[5] C. Budakoglu and T. A. Gulliver. Hierarchical key management for mobile ad-hoc networks. In *In IEEE Vehicular Technology Conference (VTC'2004)*, volume 4, pages 2735–2738.

[6] S. Capkun, L. Buttyan, and J. Hubaux. Self-organized public-key management for mobile ad hoc networks. In *ACM International Workshop on Wireless Security, WiSe*, pages 52–64.

[7] S. Capkun and J. Hubaux. Secure positioning in wireless networks. *Proceedings of IEEE JSAC, special issue on security in ad-hoc networks, 24(2), pp. 221-232, 2006*.

[8] K. Chen and K. Nahrstedt. iPass: an incentive compatible auction scheme to enable packet forwarding service in MANET. *Proceedings of the IEEE ICDCS'04, 2004*.

[9] S. Chokhani, W. Ford, R. Sabett, and C. Merill. Internet x.509 public key infrastructure certificate policy and certification practices framework. In *Internet Request for Comments (RFC3647)*, 2003.

[10] Y. Dong, H. Go, A. Sui, V. Li, L. Hui, and S. Yiu. Providing distributed certificate authority service in mobile ad hoc networks. *In Computer Communication*, 30:2442–2452, 2007.

[11] J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker. A BGP based mechanism for lowest-cost routing. *Proceedings of the ACM annual symposium on Principles of distributed computing, 2002*.

[12] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Network and Distributed System Security Symposium*, 2004.

[13] L. Hurwicz and S. Reiter. *Designing Economic Mechanisms*. Cambridge University Press, 1^{st} edition, 2008.

[14] Y. Liu, C. Comaniciu, and H. Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. In *Proceedings of the GameNets06*. ACM, Oct. 2006.

[15] A. Mas-Colell, M. Whinston, and J. Green. *Microeconomic Theory*. Oxford University Press, New York, 1995.

[16] T. VINT project. The network simulator ns-2. *http://www.isi.edu/nsnam/ns*.

[17] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya. A mechanism design-based multi-leader election scheme for intrusion detection in manet. *In the proceedings of IEEE WCNC 2008*.

[18] P. Morris. *Introduction to Game Theory*. Springer, 1^{st} edition, 1994.

[19] N. Nisan and A. Ronen. Algorithmic mechanism design. *Proceedings of STOC, 1999*.

[20] H. Otrok, M. Mehrandish, C. Assi, M. Debbabi, and P. Bhattacharya. Game theoretic models for detecting network intrusions. *In the Computer Communications journal, Volume* 31*, Issue* 10*, June 2008, pp: 1934-1944, Elsevier Press*.

[21] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya. A game-theoretic intrusion detection model for mobile ad-hoc networks. *Journal of Computer Communications, 31(4):*$708 - 721$*, 2008*.

[22] A. Rachedi and A. Benslimane. A secure architecture for mobile ad hoc networks. In *proceedings of International Conference MSN'06, LNCS*, volume 4325, pages 424–435, China, 2006.

[23] C. Satizabal, J. Hernandez-Serrano, J. Forné, and J. Pegueroles. Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks. *Computer Communication*, 30:1498–1512, 2007.

[24] A. Shamir. How to share a secret. In *Communications of the ACM*, volume 22, pages 612–613, 1995.

[25] M. Willem. *Minimax Theorem*. Birkhauser, USA, 1996.