ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Intrusion Detection and Response System in MANET Using Leader Election Based Mechanism Design Approach

B. Vaishnavi Devi[1], N. Sakthi Priya*[2]

[1]Department of Computer Science, Jerusalem College of Engineering, Chennai, India

[2]Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, India

*Corresponding Author,

ABSTRACT: A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a network without using any existing infrastructure. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. In MANET (mobile ad-hoc network), leader election takes place in the presence of selfish nodes for intrusion detection. In order to balance the resources in the nodes the nodes having the more weightage is being elected as the leader. There exist two obstacles to achieve this goal. Without any incentive being allocated, the node lies about its resources and acts selfishly by avoiding itself not being elected. Second, electing an optimal collection of leaders to minimize the overall resource consumption may incur a prohibitive performance overhead. Similarly intrusion detection system (IDS) plays major role for controlling malicious activity in the mobile ad-hoc network. Therefore assigning IDS to each and every node is time consuming process and the overall lifetime of IDS in MANET gets reduced. The efficient mechanism design approach been used in leader election based IDS to detect the malicious activities of mobile nodes and this system also leads a solution for reputation based secured communication in trusted mobile adhoc networks.

I.INTRODUCTION

Mobile ad-hoc Network is a distributed network is a self-organizing network without centralized management, in which each node functions autonomously. A mobile ad hoc network (MANET) is a distributed network. In a MANET, because of the short transmission range, a packet is forwarded in a multi-hop fashion to its destination relying on the nodes in the routing path. Thus, MANETs require the cooperation of every node in the path for successful packet transmission. Sometimes it happens that the nodes lie about their self in order to not making them responsible for the network, sometime s they may show more resources in spite of being weak and gain control of the network. In order to prevent this ,leader election and authorization using IDS intrusion detection system is being implemented in our work.

Security constraint in ad hoc routing protocols is important factor that all anticipating nodes do so in good faith and without maliciously disrupting the operation of protocol. In ad hoc network the Intrusion detection system (IDS) plays major role to monitor the malicious activities within the network. Since IDS also responsible for detecting various attacks like Black hole attack, DDos attack, Worm hole attack etc.A common approach for reducing the overall resource consumption of intrusion detection in MANET is for nodes to collaborate in electing a leader to serve as the intrusion detection system (IDS) for a cluster of one- hop nodes. The election process can be either random or based on the connectivity. Both approaches aim to reduce the overall resource consumption of IDSs in the network. However, we notice that nodes may have different remaining resources at any given time and this should be taken into account by an election scheme. With the random model, each node is equally likely to be elected regardless of its remaining resources. The connectivity index-based approach elects a node with high degree of connectivity even though the node may have little resources left.

With both election schemes, some nodes will die faster than others, leading to a loss in connectivity and potentially the partition of network. Although it is clearly desirable to balance the resource consumption of IDSs among nodes, this objective is difficult to achieve due to the presence of selfish nodes. By implementing cohesion based leader mechanism the leader node's work is shared by its cluster nodes which withstands for longer time.

A mobile ad hoc network (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the larger internet.

Mobile ad hoc networks consist of mobile hosts equipped with wireless communication devices. All hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae receive the transmission of a mobile host. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message, which effectively builds connected networks among the mobile hosts in the deployed area.

Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts.

The mobility and autonomy introduces a dynamic topology of the networks not only because end-hosts are transient but also because intermediate hosts on a communication path are transient.Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting to the internet, reading and sending E-mail messages, changing information in a meeting and so on.

There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected). This is where ad hoc networks step in.

All hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae receive the transmission of a mobile host. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their message, which effectively builds connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration.

A.Leader election mechanism in MANETs

Nodes in mobile ad hoc networks exist in infrastructure less topology so they keep moving frequently and do not have a fixed network. Thus the problem of selfishness and energy balancing exists in many other applications like in IDS scheme, leader election is needed for routing and key distribution in MANET. In key management, a central key distributor is needed to update the keys of nodes. In routing, the nodes are grouped into small clusters and each cluster elects a cluster head (leader) to forward the packets of other nodes. Thus, one node can stay alive, while others can be in the energy-saving mode. The election of a leader node is done randomly, based on connectivity (nodes' degree) or based on a node's weight (here, the weight refers to the remaining energy of a node). We have already pointed out the problems of random model and connectivity model. We believe that a weight- based leader election should be the proper method for election.

B.Mechanism design model in MANETs

Mechanism design is a subfield of microeconomics and game theory. Mechanism design uses game theory tools to achieve the desired goals. The main difference between game theory and mechanism design is that the former can be used to study what could happen when independent players act selfishly. On the other hand, mechanism design allows a game designer to define rules in terms of the SCF such that players will play according to these rules. The balance of IDS resource consumption problem can be modeled using mechanism design theory with an objective

function that depends on the private information of the players. The private information of the player is the cost of analysis, which depends on the player's energy level. Here, the rational players select to deliver the untruthful or incomplete information about their preferences if that leads to individually better outcomes. The main goal of using mechanism design is to address this problem by:
1) Designing incentives for players (nodes) to provide truthful information about their preferences over different outcomesand
2) Computing the optimal system-wide solution.

C.Intrusion detection system in MANETs

The difference between wired infrastructure networks and mobile ad hoc networks raises the need for new IDS models that can handle new security challenges. Due to the security needs in MANET, a cooperative intrusion detection model has been proposed in, where every node participates in running its IDS in order to collect and identify possible intrusions. If an anomaly is detected with weak evidence, then a global detection process is initiated for further investigation about the intrusion through a secure channel. An extension of this model was proposed in, where a set of intrusions can be identified with their corresponding sources. Moreover, this address the problem of runtime resource constraints through modeling a repeatable and random leader election framework. An elected leader is responsible for detecting intrusions for a predefined period of time. Unlike our work, the random election scheme does not consider the remaining resources of nodes or the presence of selfish nodes. In a modular IDS system based on mobile agents is proposed and the authors point out the impact of limited computational and battery power on the network monitoring tasks. Again, the solution ignores both the difference in remaining resources and the selfishness issue. To motivate the selfish nodes in routing, CONFIDANT proposes a reputation system where each node keeps track of the misbehaving nodes. The reputation system is built on the negative evaluations rather than positive impression. Whenever a specific threshold is exceeded, an appropriate action is taken against the node. Therefore, nodes are motivated to participate by punishing the misbehaving ones through giving a negative reputation. As a consequence of such a design, a malicious node can broadcast a negative impression about a node in order to be punished. On the other hand, CORE is proposed as a cooperative enforcement mechanism based on monitoring and reputation systems.The goal of this model is to detect selfish nodes and enforce them to cooperate. Each node keeps track of other nodes cooperation using reputation as a metric. CORE ensures that misbehaving nodes are punished by gradually excluding them from communication services. In this model, the reputation is calculated based on data monitored by local nodes and information provided by other nodes involved in each operation. In contrast to such passive approaches, this solution proactively encourages nodes to behave honestly through computing reputations based on mechanism design. Moreover, it is able to punish misbehaving leaders through a cooperative punishment system based on cooperative game theory. In addition to this, a non-cooperative game is designed to help the leader IDS to increase the probability of detection by distributing the node's sampling over the most critical links.

D.Integrated leader election based IDS for MANETs:

Leader election based intrusion detection system is very essential to monitor the malicious activities and also to prolong the lifetime of the MANETs. Since this integrated system helps to provide security for the MANETs by monitoring the activities and behavior of the nodes in the mobile ad hoc network. The IDS helps to provide security for the end-to-end communication of the nodes with safe packet transfer among the nodes.

II.RELATED WORKS

This chapter gives the overall description of the reference papers, through which we can identify the problems of existing methodology. Also the methods to overcome such problems can be identified.

Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi, and Prabir Bhattacharya [1] In this paper the leader election in the presence of selfish nodes for intrusion detection in mobile ad hoc networks (MANETs). To balance the resource consumption among all nodes and prolong the lifetime of an MANET, nodes with the most remaining resources should be elected as the leaders. However, there are two main obstacles in achieving this goal.

First, without incentives for serving others, a node might behave selfishly by lying about its remaining resources and avoiding being elected. Second, electing an optimal collection of leaders to minimize the overall resource consumption may incur a prohibitive performance overhead, if such an election requires flooding the network. To address the issue of selfish nodes, we present a solution based on mechanism design theory. More specifically, the solution provides nodes with incentives in the form of reputations to encourage nodes in honestly participating in the election process. The amount of incentives is based on the Vickrey, Clarke, and Groves (VCG) model to ensure truth-telling to be the dominant strategy for any node. To address the optimal election issue, we propose a series of local election algorithms that can lead to globally optimal election results with a low cost.

HadiOtrok, Lingyu Wang, Noman Mohammed, MouradDebbabi and PrabirBhattacharya , [2] This paper, we study the election of multiple leaders for intrusion detection in the presence of selfish nodes in mobile ad hoc networks (MANETs). To balance the resource consumption and prolong the lifetime of all nodes, each cluster should elect a node with the most remaining resources as its leader. However, without incentives for serving others, a node may behave selfishly by lying about its remaining resource and avoiding being elected. We present a solution based on mechanism design theory. More specifically, we design a scheme for electing cluster leaders that have the following two advantages: First, the collection of elected leaders is the optimal in the sense that the overall resource consumption will be balanced among all nodes in the network overtime. Second, the scheme provides the leaders with incentives in the form of reputation so that nodes are encouraged to honestly participate in the election process. The design of such incentives is based on the Vickrey, Clarke, and Groves (VCG) model by which truth-telling is the dominant strategy for each node. Simulation results show that our scheme can effectively prolong the overall lifetime of IDS in MANET and balance the resource consumptions among all the nodes.

Jin-Hee Cho,Ananthram Swamiand Ing-Ray Chen, [3] This paper suggests Managing trust in a distributed Mobile Ad Hoc Net- work (MANET) is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and reconfigurability. In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social, information and communication networks, and take into account the severe resource constraints (e.g., computing power, energy, bandwidth, time), and dynamics (e.g., topology changes, node mobility, node failure, propagation channel conditions). We seek to combine the notions of “social trust” derived from social networks with “quality-of-service (QoS) trust” derived from information and communication networks to obtain a composite trust metric. We discuss the concepts and properties of trust and derive some unique characteristics of trust in MANETs, drawing upon social notions of trust. We provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs

.

HadiOtrok, Noman Mohammed, Lingyu Wang, MouradDebbabi, Prabir Bhattacharya,[4] This paper addresses the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. However, most current solutions elect a leader randomly without considering the resource level of nodes. Such a solution will cause nodes with less remaining resources to die faster, reducing the overall lifetime of the cluster. It is also vulnerable to selfish nodes who do not provide services to others while at the same time benefiting from such services. Our experiments show that the presence of selfish nodes can significantly reduce the effectiveness of an IDS because less packets are inspected over time. To increase the effectiveness of an IDS in MANET, we propose a unified framework that is able to: Balance the resource consumption among all the nodes and thus increase the overall lifetime of a cluster by electing truthfully and efficiently the most cost-efficient node known as leader-IDS. A mechanism is designed using Vickrey, Clarke, and Groves (VCG) to achieve the desired goal. Catch and punish a misbehaving leader through checkers that monitor the behavior of the leader. A cooperative game-theoretic model is proposed to analyze the interaction among checkers to reduce the false-positive rate. A multi-stage catch mechanism is also introduced to reduce the performance overhead of checkers.Maximize the probability of detection for an elected leader to effectively execute the detection service. This is achieved by formulating a zero-sum non-cooperative game between the leader and intruder.

DjamelDjenouri and LyesKhelladi, Algiers NadjibBadache,This paper addresses the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, the absence of a certification authority, and the lack of a centralized monitoring or management point. Earlier studies on mobile ad hoc networks (MANETs) aimed at proposing protocols for some fundamental problems, such as routing, and tried to cope with the challenges imposed by the new environment. These proto- cols, however, fully trust all nodes and do not consider the security aspect. They are consequently vulnerable to attacks and misbehavior. More recent studies focused on security problems in MANETs, and pro- posed mechanisms to secure protocols and applications. This article surveys these studies. It presents and discusses several security problems along with the currently proposed solutions at different network layers of MANETs. Security issues involved in this article include routing and data forwarding, medium access, key management and intrusion detection systems (IDSs). This survey also includes an overview of security in a particular type of MANET, namely, wireless sensor networks (WSNs).

Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, In this paper Nodes rely on each other to store and forward packets. Most of the proposed MANET protocols assume cooperative and friendly network context, and do not address security issues. Furthermore, MANETs are highly vulnerable for passive and active attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Encryption and authentication solutions, which are considered as the first line of defense, are not sufficient to protect MANETs from packet dropping attacks. Most of the current Intrusion Detection Systems (IDSs) for MANETS rely on the Watchdog technique. In this research we study the behavior of this technique and propose a novel mechanism, named: Adaptive Acknowledgment (AACK), for solving two significant problems: the limited transmission power and receiver collision. This mechanism is an enhancement to the TWOACK scheme where its detection overhead is reduced while the detection efficiency is increased. NS2 is used to simulate and evaluate the proposed scheme and compare it against the TWOACK and Watchdog methods. The obtained results show that the new AACK scheme outperforms both of the TWOACK and Watchdog methods in terms of network packet delivery ratio and routing overhead.

III. PROPOSED SYSTEM

We proposed a system combining the intrusion detection system and the system with leader election mechanism. By integrating these systems the misbehaviorand detection of selfish and malicious nodes can be identified efficiently on comparing to the previous system model.A malicious node can disrupt our election algorithm by claiming a fake low cost in order to be elected as a leader. Once elected, the node does not provide IDS services, which eases the job of intruders. To catch and punish a misbehaving leader who does not serve others after being elected, we have proposed in a decentralized catch- and-punish mechanism using random checker nodes to monitor the behavior of the leader. Although not repeated here, this scheme can certainly be applied here to thwart malicious nodes by catching and excluding them from the network. Due to the presence of checkers, a malicious node has no incentive to become a leader since it will be caught and punished by the checkers. After a leader is caught misbehaving, it will be punished by receiving a negative reputation and is consequently excluded from future services of the cluster.

Thus, our mechanism is still valid even in the presence of a malicious node. Generally selfish nodes are nodes which tend to lie about their resources, these resources may be dealing with power, information etc. Generally any information dealing with a node is said to be its private information hence there is a high possibility of each node lying about its presence. The risk factor here is that these nodes might still be in the cluster and yet sometimes they might be selected as a leader. Then there are probabilities that the leader does not assign proper IDS to all the other nodes in the cluster thus making the cluster not a secure one and anyone can intrude into the cluster, thus making it an insecure network.

These nodes can be found by knowing its packet delivery ratio, the nodes tend to access the unauthorized information and modifies and delays the packet delivery thus proving to be a improper network. These nodes should be detected and removed from the respective cluster inorder to prevail a proper network. This can be done by broadcasting information to the neighbor nodes about the selfish nodes and providing them information about the selfish nodes present in the network and eliminating them by not passing any information to the respective selfish nodes thus resulting in the elimination of the selfish nodes[1]. Leader election based intrusion detection system is very essential to monitor the malicious activities and also to prolong the lifetime of the MANETs. Since this integrated system helps to provide security for the MANETs by monitoring the activities and behavior of the nodes in the mobile ad hoc network. The IDS helps to provide security for the end-to-end communication of the nodes with safe packet transfer among the nodes[2].

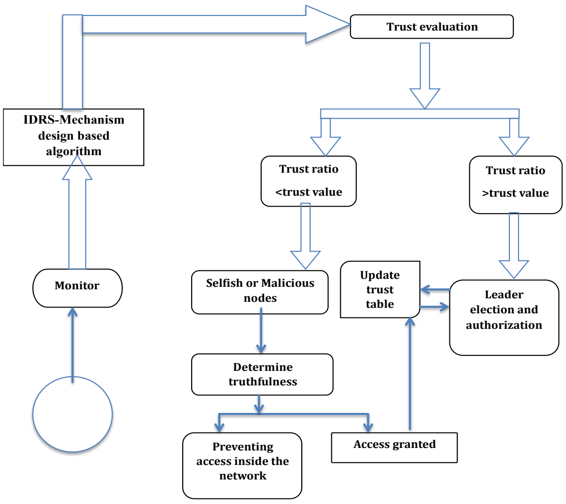

Trust evaluation
IDRS-Mechanism design based algorithm
Trust ratio <trust value
Trust ratio >trust value
Monitor
Selfish or Malicious nodes
Update trust table
Leader election and authorization
Determine truthfulness
Preventing access inside the network
Access granted

Figure 3.1 Proposed system architecture

The new node initially senses its neighborhood nodes by effective protocol such as AODV protocol[4]. Firstly it sends the route request to each of the neighbor nodes that falls within its range and waits for the route reply from these nodes. When the source node gets a reply it updates its routing table with the nodes that respond to the request thus sensing the neighbor nodes.Now the new node's trust ratio is evaluated and the node with high reputation value is elected as leader. The leader election is mainly based on the trust ratio of the nodes[5]. The IRDS mechanism based algorithm evaluates trust ratio of the node.The leader node is assigned with IDS system and then the monitoring process is initialized. Thus the leader starts the monitoring process, if the trust ratio is lesser than the threshold value means than the node is considered as selfish or malicious node and then it is removed or terminated from the network by preventing the access inside the network, if the node satisfies the trust ratio then it is allowed to reside into the network for communication by granting access[6].

AODV discovers routes as and when necessary. It does not maintain routes from every node to every other. Routes are maintained just as long as necessary. Every node maintains its monotonically increasing sequence number. Its sequence number increases every time the node notices change in the neighborhood topology
AODV utilizes routing tables to store routing information. It makes use of two kinds of routing table
1. A Routing table for unicast routes
2. A Routing table for multicast routes
The route table stores:
1.destination addr
2.next-hop addr
3.destination sequence number
4.life_time
For each destination, a node maintains a list of precursor nodes, to route through them Precursor nodes help in route maintenance (more later) .Life-time updated every time the route is used .If route not used within its life time it expires[3].

IV.IMPLEMENTATION

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

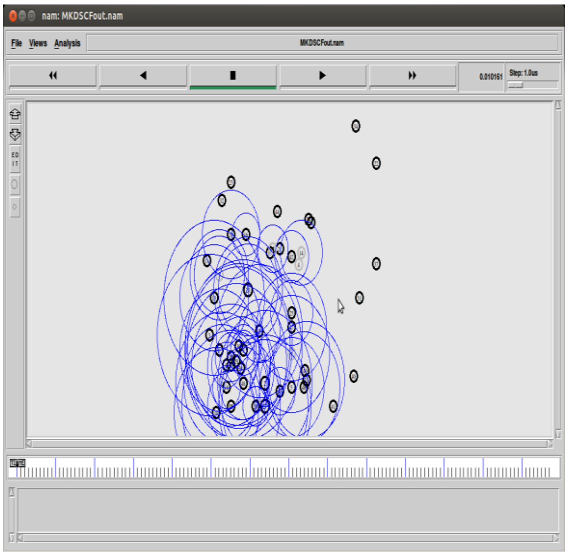
This chapter provides a detailed description of the modules in the proposed system. Implementation of the system design into a functional working model.

- Neighbourhood detection
- Leader election (cluster head)
- Assigning IDS to the cluster head
- Detection of selfish and malicious node

A.*Neighborhood detection*

Using AODV routing protocol to detect the closest neighbor to the node. The Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network[7]-[9]. It offer quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages),avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

The AODV protocol has the following features: Whenever routes are not used they get expired that is they are Discarded. This Reduces stale routes. AODV protocol reduces need for route maintenance. It also minimizes number of active routes between an active source and destination[10]-[12]. It Can determine multiple routes between a source and a destination, but implements only a single route, because it is difficult to manage multiple routes between same source/destination pair. If one route breaks, it is difficult to know whether other route is available. Lots of bookkeeping involved in this protocol.



B. Leader election mechanism

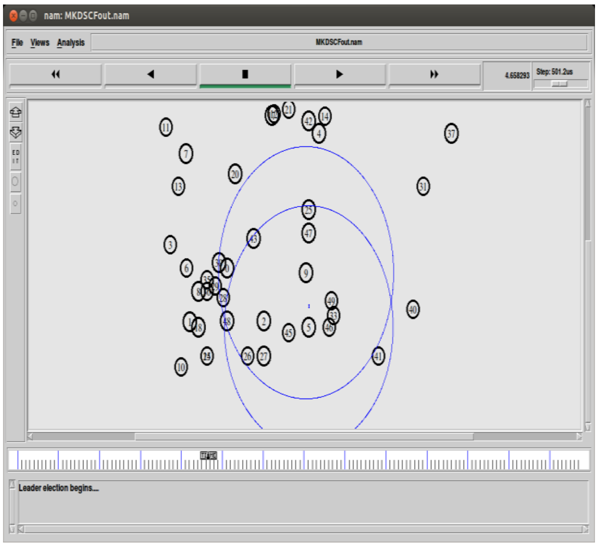
After the identification of neighborhood nodes a node with maximum number of links with other nodes is elected as leader. The election of leader is based on the leader election mechanism[13]-[15].

Mechanism design is a subfield of microeconomics and game theory. Mechanism design uses game theory tools to achieve the desired goals. The main difference between game theory and mechanism design is that the former can be used to study what could happen when independent players act selfishly. On the other hand, mechanism design allows a game designer to define rules in terms of the SCF such that players will play according to these rules. The balance of IDS resource consumption problem can be modeled using mechanism design theory with an objective function that depends on the private information of the players. In this case, the private information of the player is the cost of analysis, which depends on the player's energy level. Here, the rational players select to deliver the untruthful or incomplete information about their preferences if that leads to individually better outcomes.

The main goal of using mechanism design is to address this problem by:

1) Designing incentives for players (nodes) to provide truthful information about their preferences over different outcomes.

2) Computing the optimal system-wide solution.



Leader election begins...

C. Assigning IDS to the cluster head

After the leader election process the IDRS system is to be assigned to the cluster head and the AODV broadcast message is sent to the neighbor nodes about the currently elected leader node. And the leader starts the monitoring process[18].

D.Detection of selfish and malicious nodes

The new node's trust ratio is evaluated and the node with high reputation value is elected as leader. If the trust ratio is lesser than the threshold value means than the node is considered as selfish or malicious node and then it is removed or terminated from the network by preventing the access inside the network, If the node satisfies the trust ratio then it is allowed to reside into the network for communication by granting access. The node with maximum packet loss ratio also considers being malicious node[17]. A malicious node can disrupt our election algorithm by claiming a fake low cost in order to be elected as a leader. Once elected, the node does not provide IDS services, which eases the job of intruders.Due to the presence of checkers, a malicious node has no incentive to become a leader since it will be caught and punished by the checkers.After a leader is caught misbehaving, it will be punished by receiving a negative reputation and is consequently excluded from future services of the cluster. Hence this mechanism is still valid even in the presence of a malicious node.

E.ABOUT NETWORK SIMULATOR (NS2)

Network Simulator , widely known as NS2, is simply an event driven simulator tool that has proved useful in studying the dynamic nature of communication networks. Simulator of wired as well as wireless network functions and protocol (e.g., routing algorithm, TCP, UDP) can be done using NS2. In NS2, provides users with a way of specifying such network protocols and simulating their corresponding behaviors[16].

NS is an event driven network simulator developed at University of California at Berkeley, USA, as a REAL network simulator projects in 1989 and was developed with cooperation of several organizations. Now it is a VINT project developed by DARPA. NS is not a finished tool that can manage all kinds of network model. It is actually still an on-going effort of research and development. The users are responsible to verify that their network model simulator does not contain any bugs and the community should share their discovery with all. There is a manual called NS manual for use guidance. NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming script written by the user. There are two languages used in NS2; C++ and OTcl (an object oriented extension of Tcl).

The compiled C++ programming hierarchy makes the simulation effective and execution time faster. The OTcl script written by the users, the network models with their own specific topology, protocols and al requirements needed. The simulation results produced after running the scripts can be used either for simulation analysis or as an input to graphical software called Network Animator (NAM).

NS2 is a simulation tool; this feature is especially useful for representing thenetwork and for various calculations. It is a fully open source and can be integrated and modified. Performance, data analysis, exploration and visualization are good in NS2. Application development including graphical user interface is done effectively.

Tcl is a powerful interpreted programming language developed by John Ousterhout at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage, including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools. Nam began at LBL. It has evolved substantially over the past few years. The Nam development effort was an on-going collaboration with the VINT project. Currently, it is being developed as an open source project hosted at Source forge[14][15].

V.CONCLUSION

MANETs require all nodes in a network to cooperatively conduct a task. Encouraging this cooperation is a crucialissue for the proper functioning of the systems. Leader election and Intrusion detection are two main approachesto dealing with the cooperation problem in MANETs. In this paper, we analyze the underlying cooperation incentives ofthe two systems and a defenseless system through game theory. To overcome the observed drawbacks in each system, we propose and analyze an integrated system, which leverages the advantages of IDS. Analytical and simulation results showthe higher performance of the integrated system compared to the other two systems in terms of the effectiveness of cooperation incentives and selfish node detection.

The current system considers only about assigning the IDS to the leader node. The solution motivated nodes to truthfully elect the most cost-efficient nodes that handle the detection duty on behalf of others. To achieve this goal, incentives are given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. Reputations are computed using the well-known VCG mechanism by which truth- telling is the dominant strategy. We also analyzed the performance of the mechanisms in the presence of selfish and malicious nodes. To implement our mechanism, we devised an election algorithm with reasonable performance overheads. We also provided the algorithmic correctness and security properties of our algorithm. We addressed these issues into two applications: CILE and CDLE. The former does not require any preclustering, whereas CDLE requires nodes to be clustered before running the election mechanism.Simulation results showed that our model is able to prolong the lifetime and balance the overall resource consumptions among all the nodes in the network. Moreover, we are able to decrease the percentage of leaders, single-node clusters, and maximum cluster size, and increase the average cluster size. These properties allow us to improve the detection service through distributing the sampling budget over less number of nodes and reduce single nodes to launch their IDS.Therefore Building an efficient power managed IDS system is left as our future work.

REFERENCES

1. Noman Mohammed, HadiOtrok, Lingyu Wang, MouradDebbabi, and Prabir Bhattacharya, proposed “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011.
2. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "High data rate for coherent optical wired communication using DSP", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) 4772-4776.
3. HadiOtrok, Lingyu Wang, Noman Mohammed, MouradDebbabi and PrabirBhattacharya ,“A Mechanism Design-Based Multi-Leader Election Scheme for Intrusion Detection in MANET” Computer Security Laboratory Concordia Institute for Information Systems Engineering Concordia University, Montreal, Quebec, Canada , 2010.
4. Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
5. Jin-Hee Cho, Member, IEEE, Ananthram Swami, Fellow, IEEE, and Ing-Ray Chen, Member, IEEE, 2011.“A Survey on Trust Management for mobile ad hoc networks ”
6. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Optical ring architecture performance evaluation using ordinary receiver", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4742-4747.
7. HadiOtrok, Noman Mohammed, Lingyu Wang, MouradDebbabi, Prabir Bhattacharya Computer Security Laboratory, Concordia Institute for Information Systems Engineering, Concordia University, Montreal (QC), Canada 22 October 2007.“A game-theoretic intrusion detection model for mobile ad hoc networks”
8. Bhuvaneswari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
9. T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks”,Wireless/Mobile Network Security, Springer, 2006.
10. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Performance analysis of resilient ftth architecture with protection mechanism", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4737-4741
11. S. Vasudevan, J. Kurose, and D. Towsley, “Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks”, Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2004.
12. K. Sun, P. Peng, P. Ning, and C. Wang, “Secure Distributed Cluster Formation in Wireless Sensor Networks”, Proc. IEEE Computer Security Applications Conf. (ACSAC), 2006.
13. O. Kachirski and R. Guha, “Efficient Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks”, Proc. IEEE Hawaii Int’l Conf. System Sciences (HICSS), 2003.
14. Y. Huang, W. Lee, “A cooperative intrusion detection system for ad hoc networks”, in: Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks, ACM, Virginia, 2003, pp. 135–147.
15. MohdAnuarJaafar and Zuriati Ahmad Zukarnain, “Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment”, European Journal of Scientific Research, pp. 430-443, 2009.
16. Dr.K.P.Kaliyamurthie, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011
17. Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013
18. Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014
19. P.GAYATHRI, ASSORTED PERIODIC PATTERNS INTIME SERIES DATABASE USINGMINING, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.
20. Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013