ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Leader Election Based Malicious Detection And Response System In Manet Using Mechanism Design Approach

[1] G.Michael, [2] Dr.A.Chandrasekar
Department of Computer Science and Engineering, Bharath University, Chennai, India
Professor, St.Joseph College of Engineering, Chennai, India

Abstract: ***A Mobile Ad hoc Network (MANET) is a set of wireless mobile nodes form a network devoid of using any obtainable infrastructure. MANET is a set 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.***

Keywords: IDS,CILE,CDLE,malicious.

I. INTRODUCTION

Leader election mechanism in MANETs:

Nodes in portable specially appointed systems exist in foundation less topology so they continue moving as often as possible and don't have a settled system. In this way the issue of narrow-mindedness and vitality adjusting exists in numerous different applications like in IDS plan, pioneer race is required for steering and key dispersion in MANET. In key administration, a focal key wholesaler is expected to redesign the keys of Nodes. In directing, the hubs are assembled into little bunches and every group chooses a group head (pioneer) to forward the bundles of different hubs. In this manner, one hub can stay alive, while others can be in the vitality sparing mode. The race of a pioneer hub is done haphazardly, taking into account availability (hubs' degree) or in view of a hub's weight (here, the weight alludes to the remaining vitality of a Node). We have effectively brought up the issues of irregular model and network model. We trust that a weight-based pioneer decision ought to be the best possible strategy for race.

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. SYSTEM ANALYSIS

EXISTING SYSTEMS

To address the narrow minded conduct, they outline motivating forces as notoriety to urge hubs to genuinely take an interest in the race plan by uncovering their expense of examination. The expense of examination is intended to secure hubs' touchy data (assets level) and guarantee the commitment of each node on the decision process (decency). To rouse nodes in carrying on typically in each decision round, we relate the measure of recognition administration that every node is qualified for the nodes' notoriety esteem. In addition, this notoriety quality can

likewise be utilized to give directing need and construct a trust situation. The configuration of motivators depends on an established system outline model, to be specific, Vickrey, Clarke, and Groves (VCG). The model ensures that truth-telling is dependably the overwhelming methodology for each hub amid every race stage. Then again, to discover the internationally ideal cost-proficient pioneers, a pioneer race calculation is contrived to handle the race process, mulling over the likelihood of swindling and security defects, for example, replay assault. The calculation diminishes the rate of pioneers, single-node groups, and greatest bunch estimate, and increments normal group size. To wrap things up, they address these issues in two conceivable settings, in particular, Cluster-Independent Leader Election (CILE) and Cluster-Dependent Leader Election (CDLE). In the previous, the pioneers are chosen by got votes from the neighbor nodes. The last plan chooses pioneers after the system is detailed into various bunches. In both plans, the pioneers are chosen in an ideal route as in the asset utilization for serving as IDSs will be adjusted among all hubs additional time. At last, we legitimize the rightness of proposed routines through investigation and recreation. Em-pirical results demonstrate that our plan can successfully enhance the general lifetime of a MANET. The fundamental commitment of this paper is a bound together model that can adjust the IDS asset utilizations among all nodes by choosing the most cost-productive pioneers and to rouse childish hubs to uncover their honest assets level.

CILE Payment Design

In CILE, every nodemust be checked by a pioneer node that will investigate the bundles for other conventional hubs. Taking into account the expense of examination vector C, hubs will collaborate to choose an arrangement of pioneer nodes that will have the capacity to break down the movement over the entire system and handle the observing procedure. This expansions the productivity and parities the asset utilization of an IDS in the system. Our component gives installments to the chose pioneers for serving others (i.e., offering the identification administration). The installment depends on a for each parcel value that relies on upon the quantity of votes the chose nodes get. The nodes that don't get any vote from others won't get any installment. The installment is as notorieties, which are then used to distribute the pioneer's examining spending plan for every hub. Subsequently, any node will endeavor to expand its notoriety remembering the ultimate objective to get more IDS organizations from its relating pioneer.

Presence of Malicious Nodes

A pernicious node can upset our decision calculation by asserting a phony minimal effort keeping in mind the end goal to be chosen as a pioneer. Once chose, the hub does not give IDS administrations, which facilitates the activity of gatecrashers. To get and rebuff a getting out of hand pioneer who does not serve others subsequent to being chosen, we have proposed in a decentralized catch-and-rebuff component utilizing irregular checker node to screen the conduct of the leader.Although not rehashed here, this plan can surely be connected here to frustrate noxious hubs by getting and barring them from the system. Because of the nearness of checkers, a pernicious node has no motivator to end up noticeably a pioneer since it will be gotten and rebuffed by the checkers. After a pioneer is found getting into mischief, it will be rebuffed by accepting a negative notoriety and is therefore prohibited from future administrations of the bunch. Subsequently, our component is as yet substantial even within the sight of a pernicious node.

Presence of Selfish Nodes

For the most part egotistical nodes are nodes, which tend to lie about their assets, these assets may be managing force, data and so on. For the most part any data managing a node is said to be its private data subsequently there is a high probability of every nodelying about its vicinity. The danger element here is that these nodes may in any case be in the group but once in a while they may be chosen as a pioneer. At that point there are probabilities that the pioneer does not dole out legitimate IDS to the various nodes in the group hence making the bunch not a safe one and anybody can encroach into the group, therefore making it a frail system. These nodes can be found by knowing its parcel conveyance proportion, the nodes tend to get to the unapproved data and alters and postpones the bundle conveyance accordingly turned out to be a improper system. These nodes ought to be identified and expelled from the separate bunch keeping in mind the end goal to win an appropriate system. This should be possible by television data to the neighbor nodes about the egotistical nodes and giving themdata about the narrow minded nodes present in the system and disposing of them by not passing any data to the particular

childish nodes in this manner bringing about the end of the egotistical nodes.

III. PROBLEM STATEMENT

Security constraint in ad hoc routing protocols is important factor that allanticipating nodes do so in good reliance and lacking malignantly disturbing the process of the convention . On the other hand, the presence of malevolent hubs can't be dismissed in any framework, particularly in open ones like ad hoc networks. In ad hoc network the Intrusion detection system (IDS) plays major role to monitor the malicious activities within the network.

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 interrupt our election algorithm by claim a forgedinexpensivesequentially to be selected as a leader. Once selected, the node do not offer IDS services, which ease the job of intruder. To hold and chastisea mischievous leader who do not serve up others after being elected, we have projected in a decentralized catch- and-chastisemethod using random checker nodes to monitor the actions of the leader. even though not recurring here, this system can surely be used here to thwart malicious nodes by infectious and not including them from the network. Due to the being there of checkers, a malicious node has no enticement to become a leader since it willbewedged and chastise by the checkers. After a leader is wedged misbehaving, it will be punish by gettingaunenthusiasticrepute and is as a result excluded from outlook services of the cluster. Thus, our method is still valid even in the presence of a malicious node. Generally selfish nodes are nodes which tend to lie about thier 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. 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.

ADVANTAGES OF PROPOSED SYSTEM

- Selfish and malicious activity in nodes is reduced.
- Implementing cohesion based leader mechanism for sharing the work among the neighbor nodes.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

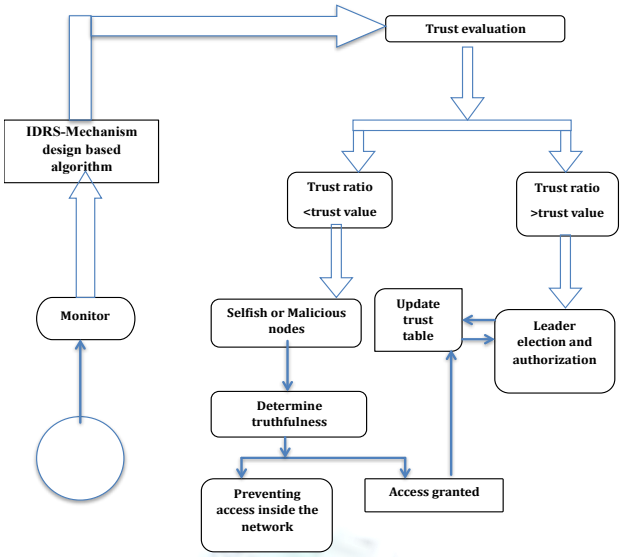

Fig .1 Proposed system architecture

The new node initially senses its neighborhood nodes by effective protocol such as AODV protocol. 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. 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.

V. IMPLEMENTATION

MODULES

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

MODULES DESCRIPTION

Neighborhood detection

Using AODV routing protocol to detect the closest neighbor to the node.The Ad hoc On-Demand Distance Vector (AODV) routing protocol isintended for use by versatile hubs in a specially appointed system. It offerquick adjustment to element join conditions, low handling andmemory overhead, low system use, and decides unicast courses to destinations inside of the specially appointed system. It usesdestination succession numbers to guarantee circle flexibility at all times (even notwithstanding strange conveyance of steering control messages),avoiding issues (such as "counting to infinity") associated withclassical 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 alsominimizesnumber of dynamic courses between anactive source and destination.ItCandetermine various courses between a sourceand a

destination, however actualizes just a singleroute, on the grounds that it is troublesome to manage multiple routes between samesource/destination pair. If one route breaks, it is difficult to know whether otherroute is available.Lots of bookkeeping involved in this protocol.

Leader election mechanism

After the recognizable proof of neighborhood hubs a hub with greatest number of connections with different hubs is chosen as pioneer. The race of pioneer depends on the pioneer race component.

Component configuration is a subfield of microeconomics and amusement hypothesis. Instrument outline utilizes amusement hypothesis devices to accomplish the fancied objectives. The principle distinction between diversion hypothesis and system configuration is that the previous can be utilized to study what could happen when free players act childishly. Then again, component plan permits an amusement originator to characterize tenets as far as the SCF such that players will play as per these principles. The equalization of IDS asset utilization issue can be displayed utilizing system outline hypothesis with a target capacity that relies on upon the private data of the players. For this situation, the private data of the player is the expense of investigation, which relies on upon the player's vitality level. Here, the normal players select to convey the untruthful or inadequate data about their inclinations if that prompts independently better results.

The fundamental objective of utilizing instrument configuration is to address this issue by:

1) Designing motivations for players (hubs) to give honest data about their inclinations over diverse results.

2) Computing the ideal framework wide arrangement.

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.

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. A malicious node can disrupt our election algorithm by claiming a forged low cost in sequence to be chosen as a leader. one timechosen, 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 gotten and rebuffed by the checkers.

After a leader is caught misbehaving, it will be punished by receiving a negative notoriety and is hence avoided from future services of the cluster. Hence this mechanism is still valid even in the presence of a malicious node.

VI. RESULTS AND DISCUSSIONS

GENERAL

The following are the results of cluster formation, neighborhood detection and leader election (cluster head) election for each cluster and assigning the IDS to the leaderdetect the egotistical and malevolent nodes in the cluster.

RESULTS

The figure .2 shows the initial stage of AODV broadcast range between the nodes.

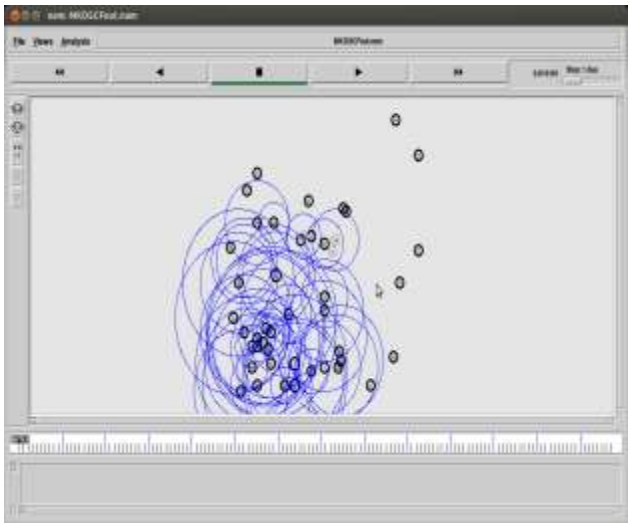

Fig .2 AODV broadcast range between the nodes

The simulation network is sensed to detect the neighborhood node by using the adhoc routing protocol.

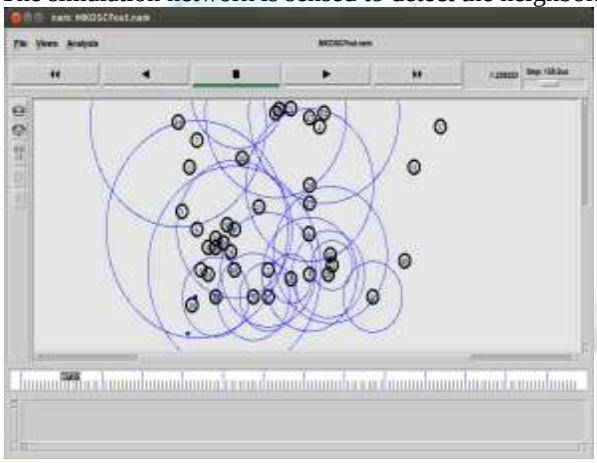

Fig .3 Neighborhood node detection

Using AODV routing protocol to detect the closest neighbor to the node.The ad hoc On-Demand Distance Vector (AODV) routing protocol is planned for use by versatile hubs in an impromptu system. It offerquick adjustment to element join conditions, low handling andmemory overhead, low system usage, and determines unicast routes to destinations within the ad hoc network.

The simulation results for electing the initial leader in the adhoc network are given below.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

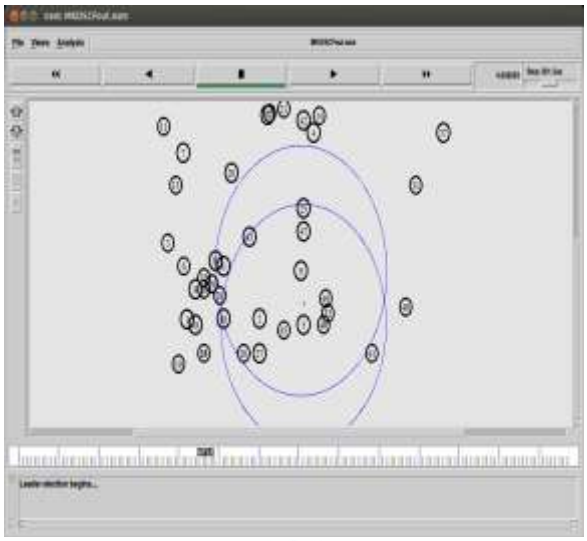

Fig .4 Initialization of Leader Election Process

Here node 9 has a good reputation and good packet transfer ratio which delivers the packets in time so it is participating for the election.

The simulation results after electing the initial leader in the adhoc network is given below

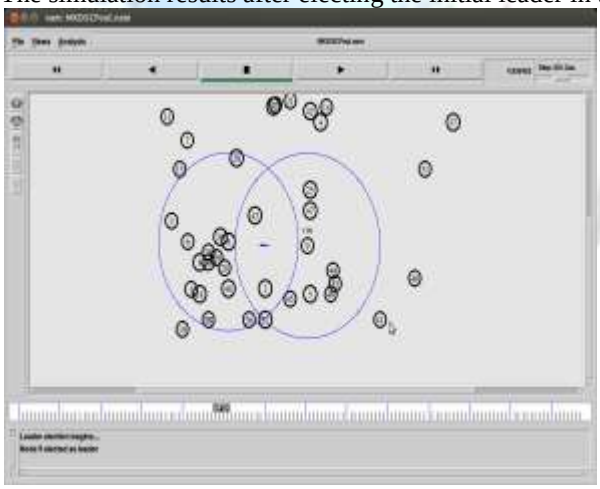

Fig.5 After electing the leader node

Based on the reputation and the links between the neighbor nodes, the node 9 is elected as the leader for the nodes [4,2,5,0], Now these nodes forms a cluster '0'.
After electing the leader IDS is assigned to the cluster head and the cluster head monitors the nodes activity.

The simulation result shows the packet-dropping instance by the node '1' given below in the figure .6.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

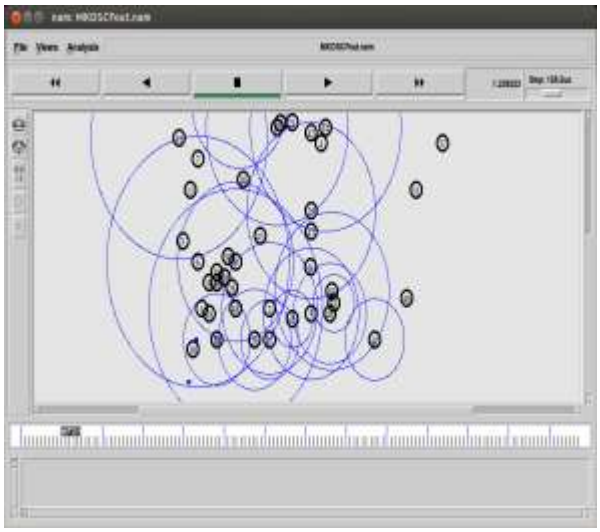

Fig .6 Packet dropping instance by the node '1'

From the above figure the packet dropping ratio of node'1' is higher, so the leader monitor's and it is said to be malicious node (refer fig.7).
The simulation results for detecting malicious node based on the packet-dropping ratio is given below in the figure .7.

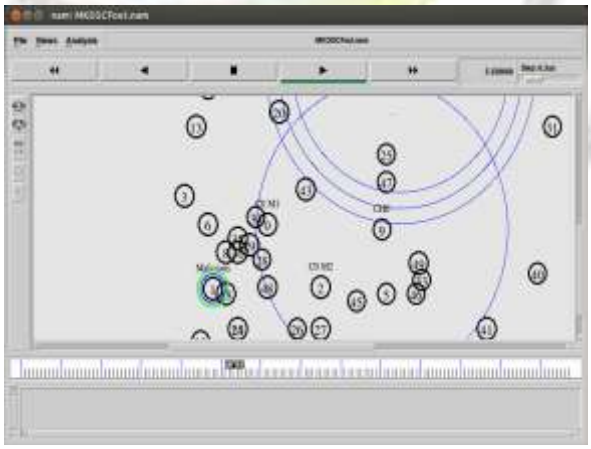

Fig .7 Detection of malicious node
The above figure shows the malicious node detection based on the packet-dropping ratio.

V. CONCLUSION

MANETs require all hubs in a system to helpfully direct an undertaking. Empowering this collaboration is a crucial issue for the best possible working of the frameworks. Pioneer decision and Intrusion recognition are two fundamental approaches to managing the collaboration issue in MANETs. In thispaper, we examine the basic participation impetuses ofthe two frameworks and an exposed framework through gametheory. To beat the watched downsides in each system, we propose and dissect a coordinated framework, which influences the upsides of IDS. Diagnostic and reenactment results show the higher execution of the coordinated framework comparedto the other two frameworks as far as the viability of cooperation motivators and narrow minded hub location.

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] 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.

[3] 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"
[4] 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"
[5] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks",Wireless/Mobile Network Security, Springer, 2006.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, Vol. 13, No.6, November/December 2008.
[12] T.A.Wysocki, A.Dadej, and B. J. Wysocki, Eds, "Secure routing protocols for mobile ad-hoc wireless networks, in Advanced Wired and Wireless Networks", Springer 2009.
[13] B. Sun *et al.*, "Integration of Secure In-Network Aggregation and System Monitoring for Wireless Sensor Networks",*IEEE ICC '07*, Glasgow, U.K., June 2007.
[14] Y. Hu, A Perrig and D. Johnson, "Packet Leashes: A Defense against Wormhole Attack in Wireless Ad Hoc Networks", in proceedings of IEEE INFOCOM'03, 2003.
[15] DjamelDjenouri and LyesKhelladi, Cerist Center of Research,AlgiersNadjibBadache,University of science and technology,Algiers, "Ile Ad hoc and Sensor Networks",IEEE communication fourth quarter 2005 Vol No 5.
[16] A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, King Fahd University of Petroleum and Minerals, Computer Engineering Department Acadia University, Jodrey School of Computer Science University of Ottawa, The School of Information Technology and Engineering,"AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement",2010 24th IEEE International Conference on Advanced Information and networking applications.