Leader election based malicious detection and response system in MANET using mechanism design approach

G. Michael[1], A. Chandrasekar[2]
[1]Department of Computer Science and Engineering, Bharath University, Chennai, India
[2]St.Joseph College of Engineering, Chennai, India
Email: micmgeo@yahoo.co.in

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 ready with both a wireless-transmitter and receiver that converse with every one via bi-directional wireless links either directly or indirectly. In MANET (mobile ad-hoc network), leader election takes place in the company 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 chosen. Second, elect a best collection of leaders to diminish the overall resource use may incur an excessive 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 on the whole lifetime of IDS in MANET gets reduced. The well-organized 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

KEY WORDS: IDS, CILE, CDLE, malicious.

1. 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 guiding and enter scattering in MANET. In key organization, a central key wholesaler is relied upon to update the keys of Nodes. In coordinating, the center points are amassed into little packs and each gathering picks a gathering head (pioneer) to forward the groups of diverse center points. In this way, one center point can stay alive, while others can be in the imperativeness saving mode. The race of a pioneer center is done erratically, considering accessibility (center points' degree) or in perspective of a center's weight (here, the weight insinuates the remaining essentialness of a Node). We have viably raised the issues of sporadic model and arrange model. We assume that a weight-based pioneer choice should be the most ideal methodology 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.

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.

2. MATERIALS AND METHODS

CILE Payment Design: In CILE, every node must 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 keeping in mind the end goal to get more IDS administrations from its relating pioneer.

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 node lying about its vicinity.[23-24] 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 an 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 those data 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.

Problem statement: Security constraint in ad hoc routing protocols is important factor that all anticipating 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 misbehavior and detection of selfish and malicious nodes can be identified efficiently on comparing to the previous system model. A malicious node can interfere with our decision calculation by case a manufactured reasonable consecutively to be chosen as a pioneer. Once chose, the hub don't offer IDS administrations, which facilitate the occupation of gatecrasher. [25-27]To hold and rebuke an underhanded pioneer who don't serve up others in the wake of being chosen, we have anticipated in a decentralized catch-and-chide system utilizing arbitrary checker hubs to screen the activities of the pioneer. Despite the fact that not repeating here, this framework can doubtlessly be utilized here to upset malicious nodes by irresistible and excluding them from the system. Because of the arriving of checkers, a pernicious hub has no allurement to end up a pioneer since it will be wedged and reprimand by the checkers. After a pioneer is wedged acting mischievously, it will be rebuff by getting an apathetic notoriety and is therefore prohibited from standpoint administrations of the group. In this way, our technique is still legitimate even in the vicinity 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 an improper network. These nodes should be detected and removed from the respective cluster in order 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.

System design:

System architecture:

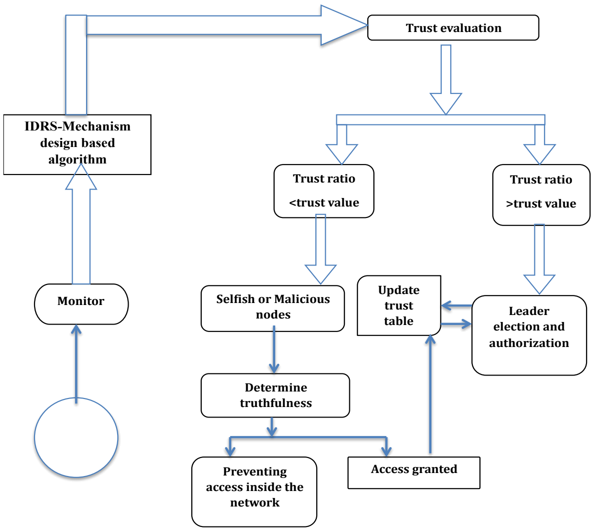

Trust evaluation
IDRS-Mechanism design based algorithm
Trust ratio <trust value
Trust ratio >trust value
Monitor
Selfish or Malicious nodes
Update trust table
Leader election and authorization
Determine truthfulness
Preventing access inside the network
Access granted

Figure.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.

Implementation:

Modules:

- Neighborhood 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 is intended for use by versatile hubs in a specially appointed system. It offer quick adjustment to element join conditions, low handling and memory overhead, low system use, and decides unicast courses to destinations inside of the specially appointed system. It uses destination 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 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 dynamic courses between an active source and destination. It can determine various courses between a source and a destination, however actualizes just a single route, on the grounds that it is troublesome 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.

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:

- Designing motivations for players (hubs) to give honest data about their inclinations over diverse results.
- 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 disturb our race calculation by guaranteeing a produced minimal effort in grouping to be picked as a leader. One time picked, the node does not give IDS administrations, which facilitates the employment of intruders. Due to the vicinity of checkers, a malicious node has no motivation to wind up a leader since it will be gotten and rebuked by the checkers. After a leader is discovered acting up, it will be rebuffed by accepting a negative reputation and is thus stayed away from future administrations of the bunch. Thus this instrument is still legitimate even in the vicinity of a malicious node.

3. 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 leader detect the egotistical and malevolent nodes in the cluster.

Results: Figure 2 shows the initial stage of AODV broadcast range between the nodes. The simulation network is sensed to detect the neighborhood node by using the adhoc routing protocol. Utilizing AODV directing convention to recognize the nearest neighbor to the node. The specially appointed On-Demand Distance Vector (AODV) steering convention is made arrangements for use by flexible center points in an off the cuff framework. It offer quick acclimation to component join conditions, low taking care of and memory overhead, low framework utilization, and decides unicast courses to destinations inside of the Ad hoc network. The simulation results for electing the initial leader in the adhoc network are given below.

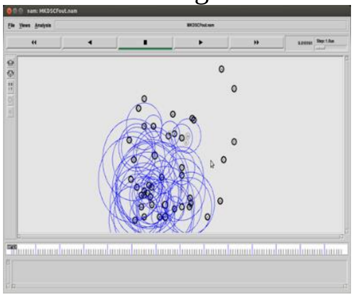


Figure.2. AODV broadcast range between the nodes

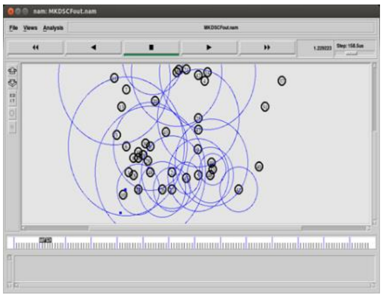
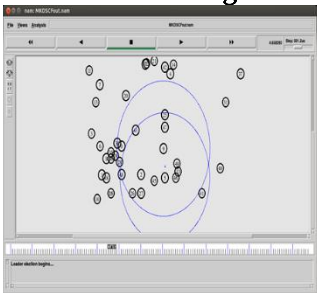
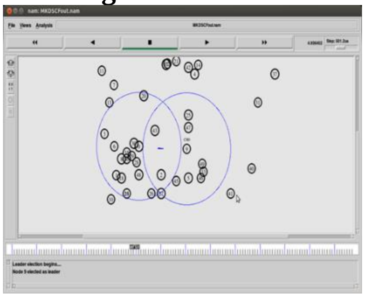


Figure.3. Neighborhood node detection



Leader election begins...

Figure.4. Initialization of Leader Election Process



Leader election begins...
Node 9 elected as leader

Figure.5. After electing the leader node

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 in figure 5. 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.

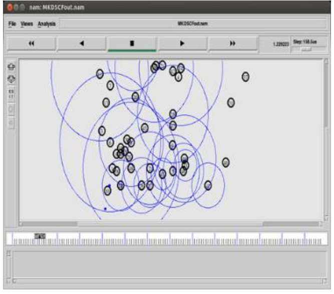


Figure.6. Packet dropping instance by the node '1'

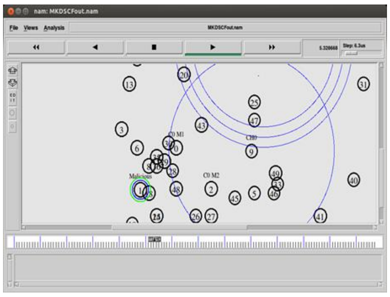


Figure.7. Detection of malicious node

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. The above figure shows the malicious node detection based on the packet-dropping ratio.

4. 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 this paper, we examine the basic participation impetuses ofthe two frameworks and an exposed framework through game theory. 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 compared to the other two frameworks as far as the viability of cooperation motivators and narrow minded hub location.

REFERENCES

Al-Roubaiey A, Sheltami T, Mahmoud A, Shakshuki E, Mouftah H, 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, 24th IEEE International Conference on Advanced Information and networking applications, 2010.

Achudhan M, Prem Jayakumar M, Mathematical modeling and control of an electrically-heated catalyst, International Journal of Applied Engineering Research, 9 (23), 2014, 23013.

Anantvalee T and Wu J, A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Springer, 2006.

Sun B, Integration of Secure In-Network Aggregation and System Monitoring for Wireless Sensor Networks, IEEE ICC '07, Glasgow, U.K, 2007.

DjamelDjenouri and LyesKhelladi, Cerist Center of Research, AlgiersNadjibBadache,University of science and technology, Algiers, Ile Ad hoc and Sensor Networks, IEEE communication fourth quarter, 5, 2005.

Gopalakrishnan K, Sundeep Aanand J, Udayakumar R, Electrical properties of doped azopolyester, Middle - East Journal of Scientific Research, 20(11), 2014, 1402-1412.

Gopinath S, Sundararaj M, Elangovan S, Rathakrishnan E, Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow, International Journal of Turbo and Jet Engines, 32 (1), 2015, 73-83.

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.

HadiOtrok, Noman Mohammed, Lingyu Wang, MouradDebbabi, Prabir Bhattacharya Computer Security Laboratory, Concordia Institute for Information Systems Engineering, Concordia University, Montreal (QC), Canada, A game-theoretic intrusion detection model for mobile ad hoc networks, 2007.

Ilayaraja K, Ambica A, Spatial distribution of groundwater quality between injambakkam-thiruvanmyiur areas, south east coast of India, Nature Environment and Pollution Technology, 14 (4), 2015, 771-776.

Jin-Hee Cho, Member, IEEE, Ananthram Swami, Fellow, IEEE, and Ing-Ray Chen, Member, IEEE, A Survey on Trust Management for mobile ad hoc networks, 2011.

Sun K, Peng P, Ning P and Wang C, Secure Distributed Cluster Formation in Wireless Sensor Networks", Proc. IEEE Computer Security Applications Conf. (ACSAC), 2006.

Kerana Hanirex D, Kaliyamurthie KP, Kumaravel A, Analysis of improved tdtr algorithm for mining frequent itemsets using dengue virus type 1 dataset: A combined approach, International Journal of Pharma and Bio Sciences, 6(2), 2015, 288-295.

Zhou L and Haas Z.J, Securing Ad Hoc Networks, IEEE Network Magazine, 13 (6), 2008.

Lingeswaran K, Prasad Karamcheti S.S, Gopikrishnan M, Ramu G, Preparation and characterization of chemical bath deposited cds thin film for solar cell, Middle - East Journal of Scientific Research, 20 (7), 2014, 812-814.

Mohd Anuar Jaafar 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, 2009, 430-443.

Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya, proposed "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET, IEEE transactions on dependable and secure computing, 8 (1), 2011.

Kachirski O and R. Guha, Efficient Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks, Proc. IEEE Hawaii Int'l Conf. System Sciences (HICSS), 2003.

Premkumar S, Ramu G, Gunasekaran S, Baskar D, Solar industrial process heating associated with thermal energy storage for feed water heating, Middle - East Journal of Scientific Research, 20 (11), 2014, 1686-1688.

Vasudevan S, Kurose J and Towsley D, Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks", Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2004.

Sundar Raj M, Saravanan T, Srinivasan V, Design of silicon-carbide based cascaded multilevel inverter, Middle - East Journal of Scientific Research, 20 (12), 2014, 1785-1791.

Wysocki T.A, Dadej A and Wysocki B.J, Eds, Secure routing protocols for mobile ad-hoc wireless networks, in Advanced Wired and Wireless Networks", Springer, 2009.

Thooyamani KP, Khanaa V, Udayakumar R, Application of pattern recognition for farsi license plate recognition, Middle - East Journal of Scientific Research, 18 (12), 2013, 1768-1774.

Thooyamani KP, Khanaa V, Udayakumar R, Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, 20 (12), 2014, 2464-2470.

Thooyamani KP, Khanaa V, Udayakumar R, Partial encryption and partial inference control based disclosure in effective cost cloud, Middle - East Journal of Scientific Research, 20 (12), 2014, 2456-2459.

Thooyamani KP, Khanaa V, Udayakumar R, Using integrated circuits with low power multi bit flip-flops in different approch, Middle - East Journal of Scientific Research, 20 (12), 2014, 2586-2593.

Thooyamani KP, Khanaa V, Udayakumar R, Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, 20 (12), 2014, 2604-2612.

Thooyamani KP, Khanaa V, Udayakumar R, Wide area wireless networks-IETF, Middle - East Journal of Scientific Research, 20 (12), 2014, 2042-2046.

Udayakumar R, Kaliyamurthie KP, Khanaa, Thooyamani KP, Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, 29 (14), 2014, 86-90.

Hu Y, A Perrig and Johnson D, Packet Leashes, A Defense against Wormhole Attack in Wireless Ad Hoc Networks", in proceedings of IEEE INFOCOM'03, 2003.

Huang Y, Lee W, 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, 135–147.