A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System

S.Tamilarasan and Dr.Aramudan

†Associate Professor, Department of Information Technology LITAM, Sattenpalli, A.P.
††Assistant Professor Department of Information Technology PKIET, Karaikal, Tamilnadu

Abstract
This paper presents a logical survey on to detect the misbehaving node in Mobile Ad hoc Network (MANET) using Intrusion Detection System (IDS). Mobile ad hoc networks have a different characteristic from wired networks and even from standard wireless networks. A mobile ad hoc network is an infrastructure less network, which is self-configuring mobile nodes connected by wireless links. There are new challenges related to security issues that need to be addressed. Due to its unique features such as open nature, lack of infrastructure and central management, node mobility and change of dynamic topology, prevention methods from attacks on them are not enough. Most of proposed MANET protocols do not address security issues. Furthermore, Mobile Ad hoc Networks (MANETs) are highly vulnerable for passive and active attacks. The Intrusion Detection is one of the possible ways in recognizing a possible attacks before the system could be penetrated. The encryption and authentication solution, which are considered as the first line of defense, are no longer sufficient to protect MANETs. Therefore, Intrusion Detection Systems (IDSs) is needed to be the second line of defense to protect the network from security problem.

Keywords:
Mobile Ad hoc Network (MANET), misbehaving node, encryption, authentication, Intrusion Detection System (IDS), decentralized property.

1. Introduction

A mobile ad hoc network (MANET) is relatively new communication paradigm. The rapid growth of wireless gadget, such as laptop, PDAs wireless sensors and Wireless phones, shows the importance of wireless technology becoming more prominent day by day [1]. The Infrastructure networks rely on a fixed base station or access point, where all the mobile nodes are connected to it. The infrastructure less networks is the ad hoc networks, where all the mobile nodes are connected to each other with the absence of an access point a centralized point of management.

A mobile ad hoc network consists of nodes. Nodes within radio range of each other can communicate directly over wireless links, and those that are far apart use other nodes as relays. Each host in a MANET also acts as a router and routers are mostly multi hop.

MANET is self –organized in such a way that a collection of mobile nodes without the help of any fixed infrastructure and central management is formed automatically [3]. Each node is equipped with a wireless receiver and transmitter that communicate with other nodes in the vicinity of its radio communication range. MANET is dynamic in nature and they constantly move in and out of their network vicinity.

Initially, MANET was designed for military applications, but, in recent years, has found new usage, For example, search and rescue mission, data collection, virtual classes and conferences where laptops, PDA or other mobile devices are in wireless communication. There are two types of MANET [4] namely open MANET and Closed MANET. In a closed MANET, all the mobile nodes cooperate with a common goal like emergency search and rescue in the natural disasters and military operation and law enforcement operation. In an open MANET, different goals share their resources in order to ensure global connectivity. Mobile ad hoc network is a vulnerable, so that MANET is subject to several attacks ranging from active interfering to passive eavesdropping due to its open medium. Since MANET is being used widespread, security has become a very important issue. The majority of routing protocols that have been proposed for MANET assumes that each node in the network is a peer and not a malicious node. Therefore, only a node that compromises with an attacking node can cause the network to fail.

The dynamic and cooperative nature of the ad-hoc routing infrastructure also imposes additional security threats. Attacks against the ad-hoc routing infrastructure may be made from external or internal nodes. Ad-hoc routing algorithms rely on node cooperation, where each node may act as a relay. Dynamic changes to the network topology make it difficult to detect if a node providing false routing information is Byzantine or is just out of sync with the topological changes. These additional security threats must be considered, when designing security mechanisms for a wireless ad-hoc network [17].

An intrusion detection system is a security system that detects inappropriate or malicious activity on a computer or

Manuscript received May 5, 2011
Manuscript revised May 20, 2011

network. IDS are used to determine if a computer network or server has experienced an unauthorized intrusion [16].

This paper is structured as follows. In section 2 we discuss about misbehaving or critical nodes in MANET. In section 3 we present the classification and different architecture of Intrusion Detection System (IDS). In section 4 we discuss the various technique proposed for preventing selfishness in MANET and finally provide a comprehensive comparisons of the methods in section 5.

2. Misbehaving Nodes or Critical Nodes in MANET

Those nodes in the network which cause dysfunction in network and damage the other nodes are called Misbehaving nodes or Critical nodes. There are two types of attacks in MANET, are passive and active attacks. A passive attack may cause, eavesdropping of data. An active attack to damage other nodes and cause disconnection in the network is called Malicious or Compromised nodes [5], [6]. An individual mobile node may attempt to benefit from other nodes, but refuses to share its own resources. Such nodes are called selfish or misbehaving nodes. A selfish node may refuse to forward data packets for other nodes in order to conserve its battery power. A selfish node [5, 6] impacts the normal network operation specifically by participation in the route discovery and maintenance process but refuse to forward data packets.

Malicious node may use the routing protocols to announce that it has the shortest route to the destined node for sending the packets. When this node receives the packets and does not send them. This kind of process termed as “Black hole” attack [13], [14]. Malicious nodes stop the operation of routing protocol by changing the routing information or by structuring false routing information called the “Wormhole” attack. As two malicious nodes create a wormhole tunnel and are connected to each other through a private link, it can be concluded that they have detour route in the network. This allows a node to create an artificial route in the current network and shorten the normal currency of routing messages in a way that the massages will be controlled by two attackers [15], [16].

Selfish node can intensively lower the efficiency of the network since they do not easily participate in the network operation. Malicious nodes can easily perform integrity attacks by changing the protocol fields in order to destroy the transportation of the packets, to deny access among legal nodes, and can perform attacks against the routing computations. Spoofing is a special case of integrity attacks with which a malicious node, due to lack of identity verification in the special routing protocols, forget the identity of a legal node. The result of such an attack by malicious nodes in the forgery of the network topology, which creates network loops or partitioning of the network. The lack of integrity and authentication in the routing protocols creates forged of false messages [8, 11, 12 and 13].

If a node participated in routes finding but does not forward a packet, it is a misleading node and misleads other nodes. But if a node does not participate in routes finding, it is a selfish node. Selfish nodes exploit the routing protocol to their own advantage, e.g., to enhance performance or save resources. Selfish nodes are unwillingness to cooperate as the protocol requires whenever there is a personal cost involved, and will exhibit the same behaviors as failed nodes, depending on what operations they decide not to perform. Packet dropping is the main attack by selfish nodes, where most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception [16].

3. IDS ARCHITECTURS IN MANET

Intrusion detection can be defined as a process of monitoring activities in a system which can be computer or a network. Intrusion detection also performs the detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. The primary assumptions of intrusion detection are user and program activities are observable. Intrusion detection system (IDS) based on capturing audit data and reasoning about the evidence in the data to determine whether the system is under attack. IDS can be categorized as network-based or host-based intrusion detection system. A network-based ID normally runs at the gateway of a network and “captures” and examines network packets that go through the network hardware interface. A host-based ID relies on operating system audit data to monitor and analyze the events generated by programs or users on the host [14], [15].

The network architecture of MANET can either be flat or multi layer with regard the application. In flat network infrastructure all nodes are considered equal whereas in the multilayer infrastructure all nodes are different. Nodes in the multilayer may be grouped into cluster, with a cluster-head for each cluster. Nodes communication between clusters is performed through cluster-head nodes. IDS are classified [16], [17] into stand-alone IDS, Distributed and Cooperative IDS, Hierarchical IDS, Mobile Agent for IDS.

3.1 Stand-alone IDSs

In this architecture, one IDS is executed independently for each node, and necessary decision taken for that node is based on the data collected, because there is no interaction among network nodes and therefore no data is interchanged. Each node has no knowledge of the position of the other nodes in the network and no alert information crosses the network. This architecture is not effective due to its limitation. They can be suitable for networks where nodes are not capable of executing IDS or where IDS has been installed. This architecture is also more suitable for flat network infrastructure. Due to the fact that exclusive node information is not enough to detect intrusions, thus this architecture has not selected in many of the IDS for MANETs [16].

3.2 Distributed and Cooperative IDSs

MANETs are distributed by nature and requires nodes cooperation. Each node cooperates in intrusion detection and an action is performed by IDS agent on it. Each IDS agent is responsible for detection, data collection and local events in order to detect intrusions and generate an independent response. Even though neighboring IDS agents cooperate with each other when there is not any convincing evidence in global intrusion detection. This architecture, which is similar to stand-alone IDS architecture, is more suitable for flat network infrastructure compared with multi-level infrastructure [1, 26].

3.3 Hierarchical IDSs

Hierarchical IDS architecture is the well developed distributed and cooperative IDS architecture and has been presented for multi-layered network infrastructure in such a way that network is divided into clusters. The cluster-heads of each cluster has more responsibilities compared to other members, For example, sending routing packets between clusters. The name multi-layer IDS is also used for hierarchical IDS architecture. Each IDS agent is performed on every member node and locally responsible for its node, for example, monitoring and deciding on the locally detected intrusions. Each cluster-head is locally in charge of its node and globally in charge of its cluster. For example, monitoring network packets and initiating a global reaction where an intrusion is detected [16].

3.4 Mobile Agent for IDSs

Mobile agents have been deployed in many techniques for IDSs in MANETs. Due to its ability of moving in network, each mobile agent is considered for performing just one special task and then one or more mobile agents are distributed amongst network nodes. This operation allows the distributed intrusion detection in the system. There are advantages for using mobile agents [15]. Some responsibilities are not delegated to every node, and so it helps in reducing the energy consumption, which is also an important factor in MANET network. It also provides for fault tolerance in such a way that if the network is segmented or some of the agents break down, they can still continue to function. In addition, they can work in big and different environments because mobile agents can work irrespective of their architecture, but these systems require a secure module that enables mobile agents to settle down. Moreover, Mobile agents must be able to protect themselves from secure modules on remote hosts.

4. Techniques proposed for detecting misbehaving Nodes in MANET

MANETs have an infrastructure less network, so that each node in MANETs is dependent on cooperation with other nodes for routing and forwarding packets. During the packet transmission, the intermediate nodes are involved for packet dispatch, but if these nodes are misbehaving nodes. They can delete or alter packets. Matri Giuli and Baker [18] performed simulation and show that only a few misbehaving nodes can reduce entire system efficiency. A few techniques and protocols detecting and confronting misbehaving nodes are available [21, 26].

4.1 Watchdog and Pathrater

Marti Giuli and Baker [18] were discussed two techniques are watchdog and pathrater that improve throughput in the MANET in the presence of selfish node or compromised node. The watchdog mechanism relies on bidirectional links. Watchdog mechanism overhears the communication medium to check whether the next-hop node faithfully forwards the packet. A buffer is maintained for recently sent packets. If the packet id is removed from the buffer when the watchdog overheard the same packet has been forwarded by the next-hop node over the communication medium. If a packet has remained in the buffer for longer than a certain timeout, the watchdog mechanism marks the next-hop neighbour of misbehaving. The Pathrater module would help in finding the possible routes excluding the selfish node.

Fig. 1 shows how the watchdog technique operates.

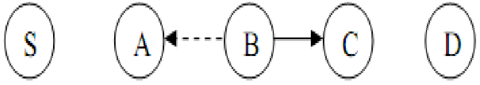


Fig. 1 Watchdog Operation

From the fig. 1, Let us assume that the nodes S (Source) wishes to send packet to node D (Destination). There exists a path from S to D via node A, B, C. Node A receives the Packet from S and forwards the packet to B. Node A keeps a copy in its buffer and then eavesdrops on node B ensuring that B forwards the packet to C. If the packet is heard by B and it is identical to what has in its buffer, this indicates that B has forwarded the packet to C. The packet is removed from the source node buffer. If a data packet remains in the buffer for too long, the watchdog module accuses the next hop neighbour of misbehaving. If the packet is not compared with the packet of the source node buffer within the specific time, the Watchdog adds one to the node B’s failure counter. If this counter exceed the threshold, node A concludes that node B is Malicious and report this to source node S. Watchdog relies upon DSR and each node takes part in the intrusion detection and response by surveillance of its downstream node, on the route form source to destination [18, 27].

Pathrater technique calculates path metric for every path. By keeping the ratings of each node in the network, the path metric can be calculated through combining the node rating with connection reliability which is obtained from previous experience. After calculating the path metric for all accessible paths, Pathrater will select the path with the highest metric. If such link reliable data with regards to the connection were not available, the path metrics would enable the Pathrater to select the shortest path. Thus it avoids routes that have misbehaving nodes [18, 32].

4.2 Confidant

The CONFIDANT protocol has been proposed by Buchegger and J.Y.Le [21]. Boudenc is similar to watchdog and pathrater. In this protocol, each node can observe the behavior of all its neighboring nodes that are within its radio range. The CONFIDANT protocol consists of the Monitor, the Reputation system, the Path Manager, and the Trust Manager. Each nodes in MANET is continuously monitor the behavior if its vicinity nodes. If a suspicious event is deleted, details of the events are passed to the Reputation system. Reputation system modifies the rating of the suspected node. If the rating of a node in the table has deteriorated so much as to fall out a tolerable range, the Path manager is called for action.

ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. The Monitor observes the next-hop neighbor’s behaviors using the overhearing technique. This causes the scheme to suffer from the same problem as the watchdog scheme. It resolves one of the problems of the watchdog that it does not use the misbehaving nodes in routing and not forward packets through them, so they are punished. When a node discovers a misbehaving node, it informs all other nodes and they too do not use this node [21].

The route is rated (good or bad) based on whether the next hop in the route belongs to the faulty list. In this scheme, every node rejects the data packets arrived from the nodes belonging to the faulty list and thus misbehaving nodes are isolated. The second chance mechanism is used to since this protocol allows network nodes to send alarm messages to each other; it is therefore a good opportunity for the attackers to send false alarm messages

4.3 Core

Michiardi and Molva [26] proposed a technique CORE (A Collaborative Reputation Mechanism to enforce node cooperation in mobile ad hoc network) similar to CONFIDANT which is based on monitoring and reputation system. In this method each node receives reports from other nodes. CORE allows only positive reports to pass through while CONFIDANT protocol allows the negative reports. The Denial of Service (DoS) attack is prevented as it does not allow the false report. In this system a negative rating is given when the node cannot cooperate and its reputation is decreased. When a positive report is received from this node the reputation rating is increased.

4.4 Ocean

The Observation-based Cooperation Enforcement in Ad hoc Network (OCEAN) has proposed by Bansal and Baker [27], which is the enhanced version of DSR protocol. In this protocol, every node maintains rating for each neighboring node and monitors their misbehavior through promiscuous mode. In this protocol, particularly tracks misleading routing misbehavior. When forwarding a packet, the module buffers the packet checksum. The OCEAN protocol monitors the behavior of the next-hop neighbor node. If it does not hear the neighbor attempt to forward the packet within a timeout (default 1ms), Neighbor Watch registers a negative event against the neighbor node and removes the checksum from its buffer. On the other hand, on overhearing a forwarding attempt by the neighbor, Neighbor Watch compares the packet to the buffered checksum, and if it matches, it treats the packet as not having been forwarded. These events are communicated to the RouteRanker, which maintains rating of the neighbor nodes.

In RouteRanker, every node maintains ratings for each of its neighboring nodes. The rating is initialized to natural and is incremented and decremented on receiving positive and negative events respectively from the Neighbor Watch component, when the absolute value of the negative decrement is larger than the positive increment. Once the rating of a node falls below a certain threshold, Faulty Threshold, the node is added to the faulty list.

The Route Request (RREQ) message of the DSR protocol has a field named avoid-list which is used to store the faulty threshold allow nodes that misbehaved in the past to become operational by assigning a neutral rating after certain period of time. Chip Count is the counter maintained by each node to track the forwarding balance with a node request to forward a packet and decreases with an incoming request from that node. The monitored node may not be able to relay the packet due to the low quality of wireless link, low battery, and network interface restart etc., Hence the second chance mechanism helps to overcome these potential problems. OCEAN is not effective in reducing the throughput of misbehaving node and takes no countermeasures to prevent collusion.

4.6 Cooperative Intrusion Detection System

Huang and Lee [2, 29, and 30] proposed a cluster-based cooperative intrusion detection system, which is capable of detecting an intrusion but also reveals the type of attack and the attacker. This type of detection is possible through statistical anomaly detection. This method uses identification rules for discovering attacks by using statistical formulas have been defined. These rules help to detect the type of attack and in some cases the attacking node. In this method hang and lee used the IDS architecture is hierarchical. In this architecture, each node has an equal chance of becoming a cluster-head. If every node in this methods are involves in monitor to detect intrusion and analyze for possible intrusion, there is a huge power consumption is occurred. Hence the cluster-head is solely responsible for computing traffic-related statistics. The energy consumption of member node is decreased as the cluster-head overhears incoming and outgoing traffic on all members of the cluster as it is one hop away. The performance of the overall network is better, decreases in CPU usage and network overhead [16]. However the detection accuracy is just a little worse than that of not implementing clusters.

4.7 ExWatchdog IDS

Nasser and Chen [25] have proposed IDS called ExWatchdog which is an extension of watchdog. Its function is also detecting intrusion from malicious nodes and reports this information to the response system (Pathrater or Routguard). Watchdog resides in each node and is based on overhearing. Thus a serious problem arises when the node that is overhearing and reporting itself is malicious, and then it can cause serious on network performance

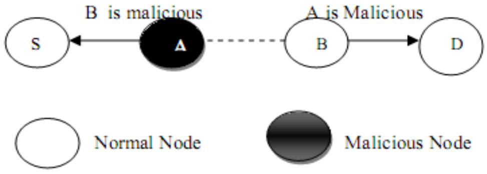


Fig. 3 Malicious node A falsely report B as misbehaving node

In the fig. 3 node A could report the node B is not forwarding packets in fact it does. This will cause S (Source) to mark B as misbehaving when A is the real culprit. ExWatchdog system is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, sum (total number of packets the currents node sends, forwards or receives) and path. Hence it can detect if nodes falsely report other nodes as misbehaving. The main feature of this system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving. This system fails when malicious node is on all paths from specific source and destination. ExWatchdog solves a fatal problem of watchdog [32].

4.8 Sori

Wu and Kholsa [31] developed a system SORI, The Secure and Objective Reputation-based Incentive Scheme for ad hoc network focus on the packet forwarding function. It consists of three basic components: neighbour monitoring, reputation propagation and punishment. Each neighbor forwarding function is linked with two parameters RFn (Request for forwarding) and HFn(x) (Has forwarded). A Local Evaluation Record (LERn (x) is created using the values of RFn(x) and HFn(x) which depicts the confidence metric. The more the packet transmitted to x for forwarding, the higher the confidence about the trustworthiness of x. In this method, the nodes exchange reputation information only with their neighbors. A non cooperative node will be punished by its entire neighbor. Each node n periodically updates LERn(x) and the respective value of its neighbor to calculate OERn(x) (Overall Evaluation Record). If the OERn(x) is lower than a predefined threshold, node n takes p punishment action by probabilistically, that the node do not intentionally drop the packets, it takes no countermeasures to prevent collision.

5. Comparison

The most of existing IDS models are in reputation scheme are based on the trustworthy, used for the forecast of future behavior [32]. The Watchdog mechanism has been used in all of the discussed IDSs [1], but has several limitations and in case of collision cannot work correctly and lead to wrongly accusation. When each node has a different transfer rang or implements directional antennas. The Watchdog cannot monitor the neighboring nodes accurately. The ExWatchdog methods solve a fatal problem of Watchdog [25].

The second chance mechanism is used to recover the node that was wrongly punished or accused, and eventually punished. OCEAN incorporates this mechanism whilst other schemes CONFIDANT implicitly address this issue. The 2ack scheme focuses on the link misbehavior and it can only work in the managed MANETs than open MANETs. CORE cannot detect malicious node misbehaviors, but SORI take no countermeasures in the collusion [31]. The table1 represents the final comparison among discussed reputation based schemes.

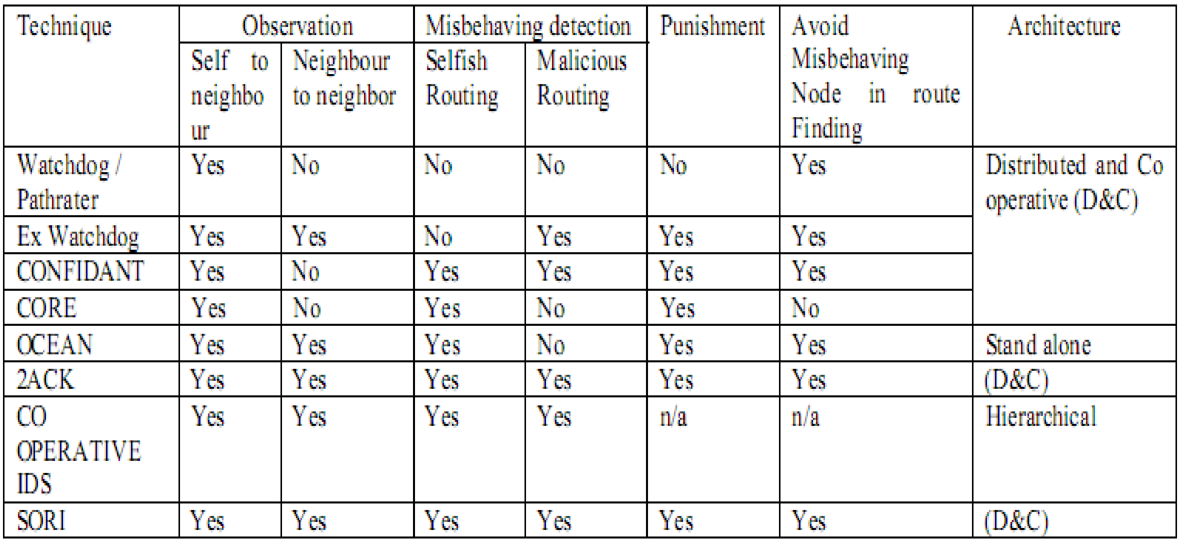
6. Conclusion

MANETs are a rapid growth of network and an area of active and prominent research over the past few years, due to its prevalent application in military defense and civilian communication. However MANETs are extremely vulnerable to attack due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication. This network is highly depends on cooperation of all of its members to achieve networking function. This makes it highly vulnerable to selfish nodes. When misbehaving nodes participate in the route discovery phase but refuse to forward the data packets, the performance is degraded severely.

Research experience has shown that avoidance techniques such as cryptography and authentication solution are first defense line, are no longer enough. Therefore intrusion detection systems have grown popular, to protect the network from the security problem. The aim of an intrusion detection system is detecting attacks on mobile nodes or intrusion into network.

Currently we are analyzing the performance of the IDS architectures and operation techniques. However many difficulties arise due to different assumption and tools that are presented by the author, of almost every scheme, simulation scenarios, parameters and variables measured vary significantly.

Table 1: Comparison of Technique Proposed for Detecting Selfishness in MANET



Technique	Observation		Misbehaving detection		Punishment	Avoid Misbehaving Node in route Finding	Architecture
	Self to neighbour	Neighbour to neighbor	Selfish Routing	Malicious Routing			
Watchdog / Pathrater	Yes	No	No	No	No	Yes	Distributed and Co operative (D&C)
Ex Watchdog	Yes	Yes	No	Yes	Yes	Yes	
CONFIDANT	Yes	No	Yes	Yes	Yes	Yes	
CORE	Yes	No	Yes	No	Yes	No	
OCEAN	Yes	Yes	Yes	No	Yes	Yes	Stand alone
2ACK	Yes	Yes	Yes	Yes	Yes	Yes	(D&C)
CO OPERATIVE IDS	Yes	Yes	Yes	Yes	n/a	n/a	Hierarchical
SORI	Yes	Yes	Yes	Yes	Yes	Yes	(D&C)

References

[1] Y.Zhang, W.Lee, and Y.Huang, "Instrusion Detection Technique for Mobile Wireless Networks" ", Proc. ACM Wireless Network 2003, ACM press 2003, pp. 545-556. Fifth Annual Conference on Communication Network and Services Research (CNSR'07) 0-7695-2835-x/07 $20.00 @2007

[2] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks ", Proc. of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks, ACM press, Virginia, 2003

[3] B. Sun and L. Osborne Young, "Intrusion Detection Techniques in mobile ad hoc and wireless sensor networks, "IEEE Wireless Communication, pp. 56-63. October 2007

[4] H. Miranda and L. Rodrugues, "Preventing Selfishness in Open mobile Ad Hoc Network, "Proc. Seventh CaberNet Radicals Workshop, Oct. 2002

[5] J. Kong, Adaptive Security for Multi-layer Ad Hoc Networks, Special Issue of Wireless Communication and Mobile Computing, John Wiley Inter Science Press, 2002.

[6] L. Blazevic, L.Buttyan, S. Capkum, S. Giordano, J. Hubaux, and J.LeBoudec, "Self-organization in mobile ad-hoc network: The approach of terminodes, IEEE Communications Magazine, Vol.39, no.6, pp.166-174, 2001

[7] Y.Zhang, and W.Lee, "Intrusion detection in wireless ad-hoc networks, "in Pro. 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 2000, pp.275-238.

[8] N. Komninoa, D. Vergados, and C. Douligeris, "Detection unauthorized and compromised nodes in mobile ad hoc networks, "Elsevier Ad hoc Network, Vol.5 no.3, pp.289-298, 2007

[9] P.Kyasanur, and N. Vaidya, "Detection and Handling of MAC layer MISbehavior in wireless networks, "Int. Conf.on Dependable Systems and Networks (DSN'03), 2003, pp.173-182

[10] Y. HU, A. Perrig, and D.B.Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, "in Proc.22th Annual Joing Conference of the IEEE

Computer and Communications Societies (INFOCOM'03), Pittsburgh, PA, USA, vol.3 2003, pp.19 76-1986

[11] P. Papadimitratos, Z.J. Haas, and E.G. Sirer, "path set selection in mobile ad hoc networks, "in Proc.3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing,Lausanne, Swizerland, 2002, pp.1-11

[12] B. Sun, W. Kui, and U.W. Pooch, "Towards adaptive intrusion detection in mobile ad hoc networks, "in proc. IEEE Global Telecommunication Conference GLOBECOM'04), Beaumont, TX, USA, vol.6, 2004, pp.3551-3555.

[13] M.K. Rafsanjani, A. Movaghar, "Identifying monitoring nodes in MANET by detecting unauthorized and malicious nodes, "in Proc.3rd IEEE Int. Symposium on Information Technolog(ITSIM'08), August 2008, pp.2798-2804

[14] Y.Huang and W.Lee, "A cooperative Intrusion Detection System for Ad Hoc Networks, "Proc. Of the 1st ACM Workshop Security of Ad hoc and Sensor Networks, ACM Press, Virginia, 2003.

[15] A.Mishra, K. Nadkari, A.Patcha and V.Tech,"Intrusion Detection in wireless Ad hoc Networks", IEEE Wireless Communication, /IEEE press, 2004.

[16] Y.Xiao, XShen and.Z.Du, Wirelesss/Mobile Network Security, Springer, 2006, Ch.7.

[17] P. Brutch and C.Ko, "Challenges in intrusion detection for wireless ad hoc networks, "in Proc., 2003 Symposium on Applications and the Internet Workshop, January 2003, pp. 368-373.

[18] S. Matri, T.Gili, K.Lai and M.Baker. "Mitigating Routing Misbehaviour in Mobile Ad hoc Network", Proc.MobiCom Aug 2000.

[19] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs, "Proc. MobiHOC, Aug.2000

[20] J.P. Hubaux, T.Gross, J.-Y. LeBoudec, and M. Vetterli, Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project, "IEEE Comm. Magazine, Jan.2001

[21] S. Buchegger and J.-Y Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks, "Pro. MobiHoc, June2002.

[22] S. Zhong, J.Chen and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks, "Proc. INFOCOM, Mar.-Apr. 2003.

[23] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, 2003

[24] A. Hasswa, M. Zulker, and H. Hassanein, Routeguard: an intrusion detection and response system for mobile ad hoc networks, Wireless And Mobile Computing, Networking And Communication 2005, P336-343, Vol. 3, August 2005.

[25] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", Proc. ICC 2007.

[26] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proc. 6th IFIP Commun. and Multimedia Security Conf., Sept. '02.

[27] S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks" , Techical Report, Stanford University, '03.

[28] Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs ", IEEE transactions on Mobile Computing ,P448-502, vol. 6, NO. 5, May 2007.

[29] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in Proc. ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003, pp. 135-147.

[30] O. Kachirski abd R.Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", in proc. 36th Annual Hawaii Int. Conf. On system Sciences (HICSS '03) January 2003, p.57.1.

[31] Q.He.D.Wu and P.Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", in Proc IEEE WCN2004, Mar'04.

[32] Marjan Kuchaki Rafsanjani, Ali Movaghar and Faroukh Koroupi," Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" in Proc of world academy of science, Engineering and Technology, Vol 34 oct '08.

[33] S.Neelavathy Pari, D.Sridharan "A Performance Comparison and Evaluation of Analysing Node Misbehaviour in MANET using Intrusion Detection System" IJCSET | Feb 2011 | Vol 1, Issue 1, 35-40

S. Tamilarasan, M.E. Associate professor cum Head of Department, Loyola institute of Technology and management, Guntur, Andhra Pradesh, India.
Specialization:

Dr.Aramudhan, M, M.E. Ph.D. Assistant Professor, Department of Information technology, Perunthalaivar Kamarajar Institute of engineering and technology, Nedungadu, Karaikal, India.