A Performance Comparison and Evaluation of Analysing Node Misbehaviour in MANET using Intrusion Detection System

S.Neelavathy Pari [1], D.Sridharan [2]

[1]*Department of Computer Technology, MIT Campus*
Anna university, Chennai, India.

[2]*Department of Electronics and Communication Engineering, CEG Campus*
Anna University, Chennai, India

Abstract— **This Paper presents a coherent survey on to detect the misbehaving node in Mobile Ad hoc Network (MANET) with the intent of serving as a quick reference to the current research issues in MANET. A mobile ad-hoc network is an infrastructure less network, that is self-configuring mobile nodes connected by wireless links. The open medium and the decentralized property of these nodes relay on each other to store and forward packets. Most of the proposed MANET protocols 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. The encryption and authentication solution, which are considered as the first line of defence, are no longer sufficient to protect MANETs. Therefore, Intrusion Detection System (IDSs) is needed to be the second line of defence to protect the network from Security problems. In recent years, the security issues on MANET have become one of the primary concerns and several existing security problem on MANET can be probed quickly for future researches.**

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

1. INTRODUCTION

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 (MANET) is a set of mobile nodes (hosts) which communicate with each other via wireless links either directly of relying on other nodes as router.

MANET is self –organized in such a way that a collection of mobile nodes without the help of an y 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. 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.

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.

In MANET decision-making, key distribution, routing, and forwarding packets, are usually decentralized and many of them depend on the cooperative participation among all the nodes. The dependency on decentralized and distributed paradigm allows an adversary to exploit new types of attacks that are designed to destroy the cooperative algorithms used in ad hoc networks. Firewalls and encryption techniques are no longer sufficient and effective for protecting ad hoc wireless network. Deploying an intrusion detection [2] and prevention system (IDS) is an important approach for MANET. An Intrusion detection system must automatically detect intrusions and consequently generate alarms in order to find an appropriate response. Detecting an unusual activity will be done through monitoring the network.

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 and damage other nodes (active attack) and cause disconnection in the network are called Malicious or Compromised nodes. 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 destined node to send packets, when the node receive the packet it does not send them. This type of attacks is termed as Black hole attack [7, 8]. Malicious nodes stop the operation of a routing protocol by changing the routing information or by structuring false routing information; this operation is called the "wormhole" attack. As two malicious nodes create a wormhole tunnel [9, 10] and are connected to each other through a private link, it can be concluded that they have a detour 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 messages will be controlled by two attackers.

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 a 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].

3. INTRUSION DETECTION SYSTEM

Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. Intrusion detection is based on a captured audit data and reasoning about evidence in the data to determine whether the system is under attack. The sources of audit data can be a keyboard input, command-based logs, application-based logs or network traffic. According to the type of audit data collected, IDS can be classified into Host-based IDS and Network based IDS [14]. Host-based IDS operate on the operating system's audit trails, system and application logs, or audit data generated by loadable-kernel modules that intercept system calls. Network based IDS operate on packet captured from network traffic. In addition, IDS may be classified on the detection technique as signature-based or misuse detection, Anomaly-based detection system and specification-based detection system [15].

Signature-based detection system: The system keeps signatures of know attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. This technique may achieve low false positive rates, but does not perform well at detecting previously unknown attacks. Like a virus detection system, it cannot detect new kinds of viruses.

Anomaly-based detection system: The normal profiles (behaviours) of users are kept in the system. The system compares the captured data with these profiles, and then deal with any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response. This system is suitable for unknown attacks but it gives high false positives rates.

Specification-based detection system: The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints. This technique [7] may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.

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.

4. TECHNIQUES PROPOSED FOR DETECTING SELFISHNESS IN MANET

The misbehaving problem and the security issues are carried on by many researchers where they have proposed many schemes [18, 19, 20, 21]. This scheme cab be broadly classified into Credit-based scheme and Reputation based scheme

3.1 CREDIT BASED SYSTEM

The vital idea of credit-based system is to provide incentives for nodes which perform faithful networking functions. Nodes get paid Incentives in the form of virtual currency or similar type of payment setup for providing services to other nodes [19, 20, 22]

L. Buttyan and J.P. HUBAUX [19] proposed the concept of nuggets or beans (Virtual Currency) to pay the node for forwarding the packets. They have proposed two models namely Packet Purse Model and the Packet Trade Model. In the Packet Purse Model, each packet is loaded with nuggets before they are sent, where each intermediate node earns nuggets for packet forwarded. In the Packet Trade Model, each intermediate node earns some nuggets and sells it to the next node for more nuggets. In this model each intermediate node earns some nuggets for providing the forwarding service. Each node maintains a counter called nuglet counter [23] which gets increased when it forward packet and decreased when the node send the packet of its own. The nuglet counter should be positive before the packet is forwarded. Thus this method helps the node in active participation in the network. This module requires a Tamper Resistant hardware to keep the nodes away from increasing the nuglet counter illegally.

Zhong et al [21] proposed SPRITE (Simple Cheat Proof Credit Based System) in which each node keeps the receipts of received / forwarded messages. When the nodes get connected to the Credit Clearance Service (CSS), each node gets its charge and Credit.

The main drawback with the Credit-Based scheme is that they require tamper-resistant hardware, internet connectivity (SPRITE) to decide the charge or credit to the node, protection for the virtual currency and payment system.

3.2 REPUTATION- BASED SCHEMES

In the Reputation Based Schemes [18, 21] network nodes collectively detect and declare the misbehaviour of the suspicious node. The declaration is propagated throughout the network so that the misbehaving node is removed from the routing from the rest of the network.

Marti et al [18] discussed two techniques namely Watchdog and Pathrater that improve throughput in the MANET in the presence of selfish node or compromised node. The watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. A buffer is maintained for the recently sent packets. A data packet id cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If the data packet remains in the buffer for a longer period, then the watchdog module 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.

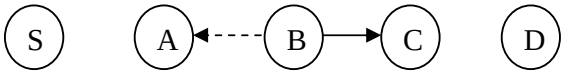

Fig. 1 Watchdog Operation

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 it 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.

Pathrater technique [18] calculates the path metric of each path and selects the path with the highest metric. 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. This method has an advantage that it can detect misbehaviour as the forwarding level and not just the link level. The weakness of the Watchdog's technique are that is might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, limited overhearing rage, collusion and partial dropping. The major weakness of Pathrater related to rating scheme are inflexible binary state, behavioural deceit, new node anonymity, re-entrance of previously malicious node and encouraging selfishness and greed. Routeguard [24] is improvement to the pathrater while assigns rating to nodes and calculates a path metric in refined way. The nodes in the network are classified into five classes namely Fresh, Member, Unstable, Suspect and Malicious. Each node is treated differently depending on its status and rating.

Nidal Nasser and Yunfeng Chen [25] developed ExWachdog an extension of Watchdog and its function is also to detect malicious nodes and report to Pathrater or Routeguard. In watchdog or Routeguard, each node updates ratings of the node according to the information provided by any node in the network. Watchdog resides in each node and depends 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.

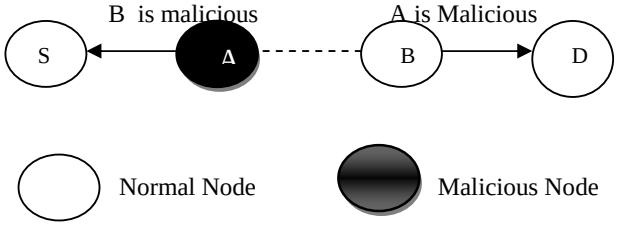

Fig. 2 Malicious node a falsely report B as misbehaving node

In the fig. 2 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.

The CONFINADT protocol proposed by Buchegger and Le Boudec [21] is similar to watchdog and Pathrater. In this protocol each node can observe the behaviour of all its neighbouring nodes that are within its radio range. CONFIDANT consists of four important components- The Monitor, The Reputation System, The Path Manager and the Trust Manager. Each node continuously monitors the behaviour of its first-hop neighbours. If a suspicious event is detected, details of the events are passed to the Reputation System. The Reputation System modifies the rating of the suspected node. Once the rating of the node become intolerable control is passed to the path manager, who controls

the route cache. Trust Manager generates the warning messages and sends to other nodes in the form of Alarm messages. The Monitor observes the next hop neighbour's behaviour 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.

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.

Michiardi and Molva [26] proposed a technique CORE (A Collaborative Repuation 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.

Observation-based Cooperation Enforcement in Ah hoc Networks (OCEAN) proposed by Bansal and Baker [27] is the enhanced version of DSR protocol. In this protocol every node maintains rating for each neighbouring node and monitors their behaviour through promiscuous mode. Positive and negative events are recorded through the reaction of the neighbour that is expected to forward the packet. Ratings are initialized to the neutral value. The value of the decrement is chosen to be bigger than the value of the increment. When the rating of the node drops below the threshold, node is added to the faulty list. The Route Request (RREQ) message of the DSR protocol has a field named avoid-list which is use 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

Kejun liu et al [28] proposed 2ACK scheme focuses the problem of detecting misbehaving links instead of misbehaving nodes. The 2ACK scheme detects misbehaviour through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

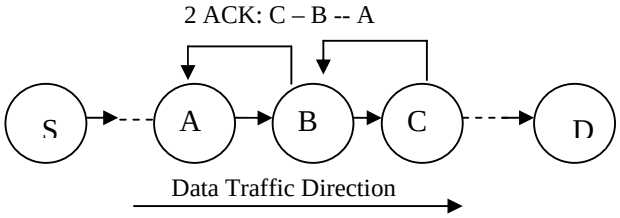

Fig 3 The 2ACK scheme

In the fig. 3 Node A, B, C are three consecutive nodes (triplet) from source node S to destination D generated in the route discovery phase of DSR protocol. When A sends packet to B, B forwards it to C. It is unclear to A whether C receives the packet successfully or not. This type of ambiguity exists even whenever there are no misbehaving nodes. The 2ACK scheme requires an explicit acknowledgement to be sent by C to notify A of its successful reception of the data packet. When node C receives the data packet successfully it sends out 2 ACK packet over two hops to A, in the opposite direction of the routing path, with the Id of the corresponding packet. Here node A monitors the link B→C. Here A is the 2ACK packet receiver or the Observing node and C is the 2ACK packet sender. This type of transmission stakes place for every set of triplets along the route expect for the first router form the source and the last router before the destination. The 2ACK scheme focuses on the link misbehaviour and it can only work in the managed MANETs as compared to open MANETs.

Huang and Lee [29, 30] proposed a cluster based cooperative intrusion detection system which is capable of detection an intrusion and reveals the type of attack and attacker. This detection is possible through the statistical anomaly detection. This method uses identification rules to detect the type of attack and the attacking node. Huang and Lee used hierarchical IDS where each node has an equal chance of becoming a cluster-head. If every node involves in monitoring and analysing the intrusion, there is a large consumption of power, hence the cluster head is responsible for computing traffic-related statistics. The energy consumption of member nodes is decreased as the cluster-head overhears incoming and outgoing traffic on all members of the cluster in a one hop away. The Performance of the overall network is better, there is a decrease in CPU usage and network overhead, however the detection accuracy is little worse than that if the system not implementing clusters.

He, 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 neighbours 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 neighbours. A non cooperative node will be punished by its entire neighbour. Each node n periodically updates LERn(x) and the respective value of its neighbour 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 collusion.

5. COMPARISON

The majority of the models in the reputation-based scheme [32] are based on the trustworthy, used for the forecast of future behaviours. Unfortunately the past behaviour can't always indicate the future behaviour. This is due to the fact that the end-systems are under the control of humans, and thus, are considered as passionate showing a not-deterministic behaviour. The Watchdog has been used on all of the IDS [1] discussed, but has several limitations and in the case of collisions can't work correctly and lead to wrongly accusation. When each node has a different transfer range or implements directional antennas, the watchdog can't monitor the neighbouring nodes accurately. The Ex-Watchdog which is designed to overcome the overhearing problem [25] of the watchdog solves the fatal problem. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impacts on network performance. 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 misbehaviour and it can only work in the managed MANETs as compared to open MANETs. CORE cannot detect malicious node misbehaviours whereas SORI [31] take no countermeasures in the collusion. Table 1 represents the final comparison among the various discussed reputation-based schemes.

The Credit-Based scheme requires tamper-resistant hardware, internet connectivity and a highly secured protection for the virtual currency and payment schemes.

Currently we are working on analysing the performance of the reputation-based models in terms of throughput improvement and to reduce the communication overheads.

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)

6. CONCLUSION

MANETs have been an area of active research over the past few years due to their potentially widespread application in military and civilian communication. However, MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security, open medium of communication. This network is highly dependent on the cooperation of all of its members to perform 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.

Researches show that cryptography and authentication solution, which are the first line of defense ,are no longer sufficient. Therefore Intrusion Detection System have grown popular, to protect the network form security problems. The aim of IDS is to detect attacks on mobile nodes.

Currently we are analysing the performance of the credit based models. The goal is to evaluate these models using a common reference scenario, however many difficulties arise due to different assumption and tools that are used for each scheme, Although simulation result are presented by the author, of almost every scheme, simulation scenarios, parameters and variables measured vary significantly.

REFERENCE

[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 TelecommunicationConference 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.