Indian J.Sci.Res. 17(2): 387-393, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

AN INTRUSION DETECTION SYSTEM FOR PREVENTION AGAINST ATTACKS IN MANET

[1] V. HarshaShastri, [2] V. Theresa Vinayasheela, [3] L. RajiniKumari
[1,2,3] Department.of Computer Science, Loyola Academy Degree and P.G College, Secunderabad, TS, India.

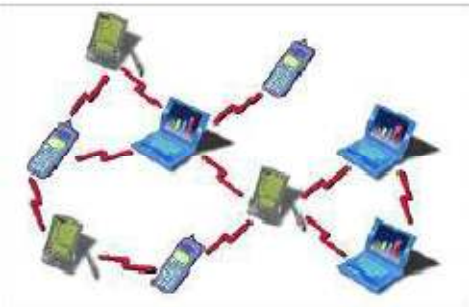
Abstract- There has been a drift from the wired network to wireless network in the past few decades. MANET is one of the most important applications of wireless network. A Mobile Ad-hoc Network (MANET) is one of the most important fields for development of wireless network. MANET is a self-configured and dynamic network that is formed by collecting number of mobile nodes. A cluster is a group of nodes. A node can be laptops, mobiles, sensors etc. A MANET is an emerging technology and can be applied in critical situations in military battle fields and commercial applications such as building traffic systems. It is infrastructure less with no central authority. The open medium and the decentralized property of these nodes relay on each other to store and forward packets. But most of the protocols do not address security issues. MANETs are vulnerable to active and passive attacks because of their open medium, dynamic topology and lack of centralized monitoring. To prevent from such intrusions we need a system which will detect as well as prevent. The authentication solution and encryption are no longer sufficient to protect against MANET. There are many security attacks in MANET and DDOS (Distributed Denial of Service) attack is one of the most important attacks. Therefore the IDS (Intrusion detection scheme) are the line of defense to protect the network from security problems.

Keywords: IDS, Watchdog, TWOACK, MANET, Attack.

I. 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]. MANET is an autonomous system in which nodes are connected by wireless links and send data to each other. Mobile Ad-hoc network (MANET) is one of the developments seen in the wireless networks. As the popularity of mobile device and wireless network significantly increased over the past years, wireless Ad-hoc network has become one of the most vibrant and active field of communication and networks. MANET is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.,) that communicate with each other over wireless links and cooperate with each other in order to provide the necessary network functionality in the absence of a fixed infrastructure. All mobile nodes are connected to each other with the absence of an access point; centralized point of management [3]. Each node is equipped with a wireless receiver and transmitter that communicate with other nodes in the vicinity of its radio communication range. There are two types of MANET: closed and open. In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/ rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. MANET consists of two types of networks, one is single hop and another is multi-hop. In a single hop network, all nodes within the same range communicate directly with each other while in a multi-hop network nodes rely on other intermediate nodes to transmit out of their radio range.

MANET is dynamic in nature and they constantly move in and out of their network vicinity. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Topology used can be mesh, star or bus for transmitting the information. While transmitting information with other node there may be a chance of getting contact with the malicious node. The figure 1 shows the MANET architecture:



[1]Corresponding Author

Figure 1: MANET architecture

II.Critical Nodes InManet

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 node may attempt to benefit from other nodes but refuses to share its own resources. Such nodes are selfish nodes. They may refuse to forward data packets for other nodes in order to conserve the battery power. A selfish node [5, 6] impacts the normal network operation 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 to send packets, when the node receives the packet it does not send them. This is a black hole attack. Malicious node stops the operation of routing protocol by changing the routing information or by structuring false routing information. This operation is a wormhole attack. The malicious nodes create a worm link tunnel [9, 10] and are connected to each other through private link. 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. Malicious nodes can easily perform integrity attacks by changing protocol fields in order to destroy the transportation of packets, to deny access among legal nodes and can perform attacks against the routing computations.

Spoofing is a special case of integrity attack with which a malicious node, due to lack of identity verification in the special routing protocols forget the identity of the legal node. The topology gets forged which creates network loops or partition of the network. The lack of integrity and authentication in the routing protocols creates forged of false messages [8, 11, 12 and 13].

III.Intrusion Detection System

Security is one of the major concerns. Intrusion Detection System (IDS) is one of the processes which monitor the activity in a systemwhich can be a computer or network and analysis them for possible intrusion. Intrusion is any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. An IDS is software that facilitates the intrusion detection process, initial responsibility of the IDS is to detect undesirable and intruder activities. It is a defensive mechanism in the MANET which provides the secured communication between the nodes. The figure 2 shows the IDS architecture.

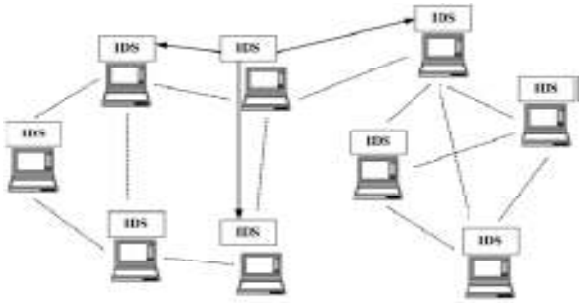


Figure 2: IDS architecture

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 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 operated 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 the 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 known 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 behaviors of the 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 positive rates.

Specification-based detection system: The system defines a set of constraints that describe the correct operation of a program or protocol. It then 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 false positive rate.

IV.IDSForManets

The attackers will leave a chance to achieve a significant effect on the network with just one or two compromised nodes. If MANET can detect the attackers as they enter the network, we will be able to delete the damages created by those successive nodes. There are some approaches, namely Watchdog, Adaptive and Acknowledgment (AACK), TWOACK, OCEAN, CORE, CONFIDANT, and EACK

A.Watchdog

Marti, Giuli, Lai and Baker [6] described the two techniques that increase the throughput in the presence of nodes that agree to forward the packets but fail to do so. The techniques are Watchdog and Pathrater. In watchdog, suppose S send data to D, then all the intermediate nodes stores packets in the buffer. If the packet remains with the node more than the timeout value then failure tally is incremented by Watchdog. Then if the failure tally increases than the threshold value then Watchdog detects node as malicious node and sends message to the source. Watchdog increases the throughput of network to 27% but increases the network overhead to 24% from 17%. Watchdog identifies the misbehaving nodes and Path rater avoids the routing through these nodes. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

To overcome the weakness of Watchdog and Pathrater, Nasser and Chen introduced intrusion detection system called ExWatchdog [2]. Through overhearing, each node can detect the malicious action of its neighbors and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. The main concern here was to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Route guard assigns ratings to nodes and calculates a path metric in a refined way. If the real malicious node is on all paths from specific source and destination, then it is impossible for the source node to confirm with the destination of the correctness of the report. It decreases network overhead. Parker presents network intrusion detection mechanisms that uses snooping algorithm to detect misbehavior in the mobile ad-hoc networks. Two response mechanisms are used - Passive to detect if node is intrusive and protects itself from attacks and Active to detect if node is intrusive and act to protect all nodes from attacks. A mis-route cannot be determined but any modification and packet dropping can be identified and locked.

Suppose there exist a path from node S to D through intermediate nodes A, B and C. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. Figure 3 illustrates how the watchdog works. When B forwards a packet from S towards D through C, A can overhear Bs transmission and can verify that B has attempted to pass the packet to C. The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer. The figure 3 shows the working of Watchdog.

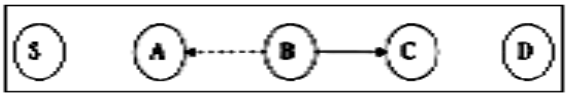


Figure 3: Working of Watchdog.

B.Two ACK

TWOACK proposed by Liu et al. [4] detects misbehaving links by acknowledging every data packet trans-mitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

The working process of TWOACK is shown in Figure 4. Node A first forwards Packet 1 to node B, and then, node

B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

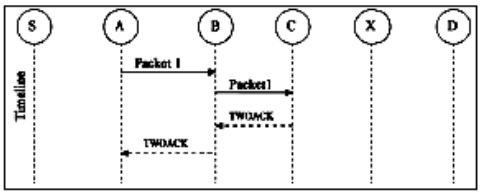


Figure 4: Working of Two ACK

C.AACK Scheme

Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called Acknowledge (ACK). Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. They fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

In the ACK scheme shown in Figure 5, the destination node is required to send back an acknowledgment packet to the source node when it receives a new packet, the source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet.

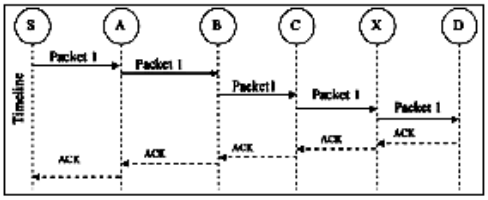


Figure 5: Working of AACK scheme.

D.EACK Scheme

To remove maximum problem of watchdog which cannot be solved by previous methods the new Enhanced AACK (EAACK) scheme [2] is developed and evaluated through implementation. It solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report. It detects the malicious nodes by verifying ACK packets. Security is not provided over here for ACK packets. Hence, there is possibility that ACK packets is misused or not send from intended receiver. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

1.ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Within a predefined time period, if node S receives Packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

2.S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [4]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode was to detect misbehaving nodes in the presence of ambiguous collision, receiver collision or limited transmission power.

3.MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers

to falsely report innocent nodes as malicious. This attack can be fatal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through different route.

E.Digital Signature

Digital signature is an important section of cryptography. Cryptography deals with the study of mathematical techniques that are related to characteristics of information security that is confidentiality, integrated data and evidence. Digital signature is a widely used approach to ensure the confirmation, integrity, [2] and non-denial of MANETs. Digital signature schemes are being divided into the following two categories.

1) Digital signature with supplementary information: In this original message is essential in the signature verification algorithm. Examples it include DSA.

2) Digital signature with message recovery: In this type of scheme it does not occupy any other information besides the signature itself will do verification of process. Examples it include RSA.

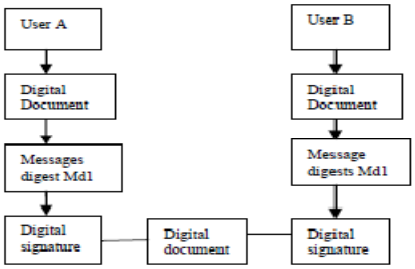


Figure 6: Digital Signature

F.CONFIDANT protocol

The CONFIANDT protocol proposed by Buchegger and Le Boudec [15] is similar to watchdog and Path rater. In this protocol each node can observe the behavior of all its neighboring 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 behavior of its first-hop neighbors. 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 neighbor's behavior 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.

G.CORE

Michiardi and Molva [16] 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.

H.OCEAN Protocol

Observation-based Cooperation Enforcement in Ad- hoc Networks (OCEAN) proposed by Bansal and Baker [20] is the enhanced version of DSR protocol. In this protocol every node maintains rating for each neighboring node and monitors their behavior through promiscuous mode. Positive and negative events are recorded through the reaction of the neighbor 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 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.

I.Cluster based Co-operative Intrusion detection System

Huang and Lee [18, 19] 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 analyzing 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 clusterhead 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.

V.Comparison

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 neighboring nodes accurately. The Ex-Watchdog which is designed to overcome the overhearing problem [17] 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 misbehavior and it can only work in the managed MANETs as compared to open MANETs. CORE cannot detect malicious node misbehaviors.

VI.Conclusion

MANETs have been an active research over the past few years due to their widespread application in military and civilian communication. MANETs are extremely vulnerable to attacks due to their dynamic topology, absence of conventional security, open medium of communication. To perform the required networking function, all the members have to cooperate. This makes it highly vulnerable to malicious nodes. The performance can be degraded if the malicious nodes refuse to forward the packets. Intrusion detection system has grown popular to protect the network from security problems. The aim of IDS is to detect the attacks on mobile nodes. Currently work is on analyzing the performance of all the approaches in terms of throughput improvement and reduces communication overheads.

Acknowledgment

The authors would like to thank the Principal Rev Fr.Dr.P. Anthony SJ for his continual support in publishing the papers. This paper would not have been completed had it not been the members of the department for their continual encouragement and support.

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] N. Kang, E. Shakshuki, and T. Sheltami, which inform us regarding "Detecting malicious misbehavring of nodes in MANETs., was held in Paris, France.

[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] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ―An Acknowledgment-based Approach for the Detection of Routing Misbehavior

in MANETs‖, IEEE Transactions on Mobile Computing, May 2007

[5] Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634-640, 20-23 April 2010.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu.Int. Conf. Mobile Comput.Netw., Boston, MA, 2000, pp. 255–265.

[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] 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.

[16] 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.

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

[18] 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.

[19] O. KachirskiabdR.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.

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