*International Journal of*
*Emerging Research in Management &Technology*
*ISSN: 2278-9359 (Volume-5, Issue-7)*

**Research Article**

**July 2016**

# Secured Intrusion Detection System in MANET

**Dipali S. Patil**
ME Student, Computer, SSBT's COET, NMU, Jalgaon,
Maharashtra, India

***Abstract—***

***From past few years, wireless networks are mostly preferred because of its scalability and mobility characteristics. Mobile Ad hoc network (MANET) is one of such wireless communication mechanisms. The self-configuring ability of nodes in MANET makes it popular among mission critical applications. The wide distribution of nodes and open medium makes MANET vulnerable to malicious attacks. It demands for more secure intrusion detection system. The EAACK intrusion detection system solves the limitations of receiver collision, limited transmission power and false misbehavior report of earlier system. EAACK uses DSR routing protocol for network of small scale. EAACK is enhanced using the concept of trust. A monitor node is placed in each link of data transmission to monitor the routers behavior. As the detection of malicious nodes is done by both EAACK and behavior checking mechanism via monitors, reduce the trust value of the malicious nodes, and the information is conveyed about the malicious node to entire network. Malicious node is not allowed in further transmission by other nodes in the network.***

***Keywords— MANET, EAACK, Trust.***

## I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is a group of autonomous mobile nodes or devices connected with the links which are wireless without the support of a communications infrastructure. The dynamism in network topology is supported as nodes move and reorganize themselves to enable communications with nodes beyond their range of wireless communications by depending on messages from one another, i.e. multihop. MANET works and depends on the cooperation of all the nodes involved. The more nodes cooperate to transfer traffic, the more powerful a MANET will be. But supporting a MANET is a costly activity for a mobile node. Finding routes and forwarding of packets consumes network-bandwidth, energy , local CPU time and memory . Therefore there is a strong motivation for a node to not to do packet forwarding to others, while at the same time using their services to deliver own data.

In contrast to traditional wired or wireless networks, MANET does not require a pre existing infrastructure or a central station. Thus, the mobile nodes inside the network move freely and randomly. This feature is of great importance when it comes to some mission critical areas like military application or disaster recovery. In such circumstances, it is usually not worthwhile or feasible to deploy fixed infrastructure centralised network. MANETs are able to construct dynamically, short lived and self-configuring network without the need for centralized network infrastructure. Minimum configuration and fast deployment make MANETs suitable for using in emergency circumstances where an

infrastructure is not available or is not feasible to install like human-induced or natural disasters, military convicts and medical emergency situations.

An individual mobile node may attempt to benefit from other nodes, but refuses to share its own resources. Such kind of nodes are known as selfish or misbehaving nodes, and their behaviour is termed selfishness or misbehavior. Wireless transmission is one of the major sources of energy consumption in mobile nodes of MANETs. A selfish or malicious node may be ready to forward control packets while drop all or part of the data packets it received to conserve its energy. Such type of attacks is termed as Denial of Service or black hole attack.

To alleviate the effects of such selfish or malicious nodes in MANETs, many researchers worked and brought proactive security approaches like cryptography and authentication to increase the security level of MANETs. However, all of these security mechanisms suffer from the problem of late detection of attacks which are malicious. This kind of flaw leaves attackers plenty of time to defect the network performance. To address this issue, it is important to use or incorporate Intrusion Detection System(IDS) into MANETs. IDS in MANETs can act as a next layer of prevention. It can work as a great complement to the existing prevention techniques. MANETs present a number of unique issues for IDS. Differentiating between malicious network activity and spurious but typical problems concerned with an ad hoc networking environment, is a challenging task. In an ad hoc network, malicious nodes may enter and exit the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network function and avoid detection. Malicious nodes may operate maliciously only intermittently, further complicating their detection.

**Mobile Ad hoc Network Characteristics:**

Some important characteristics of Ad hoc network are listed below:

1. Multi-hopping: A network where the path from source to destination traverses several other nodes .Ad hoc networks often have multiple hops for obstacle negotiation, spectrum reuse, and energy conservation-Bandwidth constrained.

 

2. Self-organization: The ad hoc network automatically determine its own configuration parameters including: addressing, position identification, power control, routing and clustering etc.
3. Variable capacity links: Wireless links have very less capacity than their hardwired counterparts. In addition, the realized throughput of wireless communication is often much less than a radio's maximum transmission rate, due to fading, noise, interference conditions, etc.
4. Energy-constrained operation: Most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply and no capability to generate their own power (e.g. solar panels).Nodes in a MANET rely on batteries, For these nodes, the most important system design parameter for optimization may be energy conservation.
5. Dynamic network topology: Nodes are free to move arbitrarily; thus, the network topology changes randomly and fast at unpredictable times. Rapid deployment in this area without infrastructure.
6. Limited Physical Security: Mobile wireless networks are generally more prone to physical security threats with compared to wired networks. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully take in to consideration.
7. Scalability: In MANETs, it is much harder to achieve scalability, but in some applications (e.g.large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc) the ad hoc network can grow to several thousand nodes.

**Mobile Ad hoc Network Security**

Security is most important for MANET because of its distributed architecture and no centralized monitoring techniques and also lack of physical protection. The MANET's securities are categorised in different ways .
1. Routing security:-The recurrent changes in the network make it very diffcult to maintain a consistent path from source to destination. One of key feature of MANET is their multi-hopped routing feature. Nodes are neede to route their packets through may be unknown nodes. Intermediate nodes can add, modify, delete or unnecessarily delay the packet forwarding. Consider the example, in DSR like source routing protocols, a malicious intermediate node can temper the source route during route discovery and maintenance phase. Hence, several types of attacks are possible during route discovery, maintenance and packet forwarding phase. So that security is necessary for secure routing in MANET. Various network intrusion detection systems have been proposed that detects malicious actions on the network and isolate the identified intruders on the network.
2. Data Forwarding Security:-In this type cryptography can help to prevent malicious attack but detection of eavesdropping is still an research topic. Also one node drops other nodes packets to preserve its resources, e.g. battery power. So that security is important for data forwarding in MANET.
3. Link Layer security: - The Key enabler for MANET is IEEE 802.11. However, the vulnerabilities associated with this standard can be led for different types of security attacks. Consider the example, the malicious node can exploit the xponential
back off feature of IEEE 802.11 protocol by continuously sending the data on the medium. This makes the medium busy and other nodes don't get opportunity to send their data. Intrusion detection system running at the link layer and monitoring for misbehaviours can also solve some of the security attacks at the link layer.
4. Key Management: - Key management is the process of establishing and maintaining of keying relationship among the entities of the network. Because of lack of any central infrastructure of MANET, there are no prior PKI servers available that can generate public and private keys for the entities of the network.
5. Intrusion Detection System: - Intrusion Detection Systems (IDS) are the second line of defence as once an intruder has entered into the system after breaking the primary security mechanisms. An intrusion is defened as any type of activity considered that attempts to compromise the security objectives. An IDS is defined as a system consist of the mechanisms intended to find an intrusion, identify the source of intrusion and then remove this source from the network. Similar to other security issues, designing IDS solution for MANET is a complex job. MANETs are more prone to attacks than traditional wired networks due to the open medium, dynamically changing network topology, cooperating algorithms, absence of centralized monitoring and lack of a clear line of defense. Most current ad hoc routing protocols manage well with the dynamically changing topology. A commonly observed misbehavior is packet dropping. These misbehaved nodes are very hard to identify because of whether the packets are dropped intentionally by the misbehaved or malfunctioned nodes or dropped due to the node moved out of transmission range or other link error. In such case, it is very necessary to develop an intrusion-detection system (IDS) specially designed and enhance the security level of MANET's. An intrusion detection system does not include preventing the intrusion from occurring, it can only be detected and reported to each node in network.

**Intrusion Detection System**

Intrusion detection system (IDS) is a system that determines whether a process or user performs violations of a security policy. For that, IDS monitors the activities on a particular machine or network and uses this data to decide whether the activity is normal or suspicious. There are three essential parts of IDS as data collection, detection, and response. The data collection component is responsible for collection and pre-processing data tasks, moving data to a common format, data storage and sending data to the detection module. IDS can use different data sources as inputs to the system such as system logs, network packets, etc. In the detection input source of data is analyzed to find intrusion attempts and indications of detected intrusions are sent to the response component. Response component is responsible for manage and using the response actions to the intrusion. Intrusion detection can be classified as either host-based or network-based. A network-based IDS captures and analyzes network traffic packet while a host-based IDS uses operating system or application logs in its analysis.

 

## II. LITERATURE SURVEY

Misbehaving node intrusion detection techniques are classified as credit based, reputation based and acknowledge based scheme.

1. Credit based scheme: The basic idea of credit based schemes is provide incentives for nodes to truly perform networking functions. To achieve this goal, electronic currency or related payment system may be used. Nodes are paid for providing services to another nodes. When they request other nodes to help them for forwarding packet, they use the same payment system to pay for such services.

Buttyan and Hubaux in[14], used the concept of nuggets (beans) as payments for for- warding packets. Two models were proposed- the Packet Purse Model and the Packet Trade Model. With the Packet Purse Model, before sending the packet nuggets are loaded. Certain number of nuggets are inserted on the data packet intended to sent by the sender. Each intermediate node earns nuggets in return of forwarding of packet. If the packet looses its nuggets before reaching destination, then it is dropped. In the Packet Trade Model, each intermediate node takes the packet with charge of some nuggets from the last node and gives it to the next node for more nuggets. Hence , every intermediate node earns some pro_t in terms of nuggets for giving the forwarding service and the overall cost of sending the packet is born by the destination.

Zhong et al. in [15], proposed the concept of Sprite. In that nodes keeps records of the received or forwarded messages. When nodes have a fast connection to a Credit Clearance Service (CCS), all of these receipts are reported. The CCS evaluates the charge and credit for the reporting nodes. In the network architecture of Sprite, the CCS is supposed to be reachable through the use of the Internet, limiting the utility of Sprite. The major issue concerned with credit-based schemes is that they usually need some kind of tamper resistant 2. Reputation Based Scheme: The second category of scheme is to conflict node misbehaviour in MANETs is Reputation based. In such schemes nodes in the network together find and declare the misbehaviour of a suspicious node. Such a declaration is then reported throughout the network so that the misbehaving node will be removed from the rest of the network.

Buchegger and Le Boudec in [16], proposed CONFIDENT protocol. It is based on selec- tive altruism and utilitarianism, which makes misbehavior unattractive. CONFIDENT has four important parts which are Monitoring system, the Reputation System, the Path Man- ager, and the Trust Manager. They carry out the most important functions of neighbourhood watching, rating of node and path and to and from of alarm messages. Each node con- tinuously looks the behavior of its first-hop neighbors. If a apprehensive event is detected, details of the process are conveyed to the Reputation System. Depending on importance and frequency of the event, the Reputation System changes the rating of the misbehaving node. As the node's rating becomes intolerable, path manager gets the control. Route cache is accordingly controlled by the path manager. Messages for warning are passed to other nodes in the form of an alarm message. The trust manager sends the alarm messages [14]. In the CONFIDENT scheme, Monitor part observes the next hop neighbor's behavior using the overhearing technique. But this leads to suffer from the same problems as the watchdog scheme.

3. Acknowledgement Based Schemes: Acknowledgement based intrusion detection system is dependant on the reception of an acknowledgment from a mobile node to check that a packet has been forwarded to it or not. The nodes in the MANETs help each other because of its characteristics. This creates a loop hole for the attackers to enter into the network and make changes in the whole network. It is always better to find the nodes malicious behaviour immediately after entering the network. With the detection of the intruders at the start, the damage to the network can be reduced to a greater extent. Hence an Intrusion Detection System is a important and should be included in any network. In the communication process of MANETs the intrusion detection system works as second layer of defence where as the routing protocol will be thefirst layer. Many researchers has worked and proposed many acknowledgements based intrusion detection schemes. Among them three main schemas discussed below.

S. Marti et. al. in [17], proposed a Watchdog scheme of intrusion detection system for MANET's. Its aim is to improve the throughput of network in the presence of malicious nodes [12]. It compromises of two parts as watchdog and pathrater. Watchdog can detect malicious nodes instead of malicious links. The watchdog is works on reactive feedback which is overheared to confirm whether the next node has forwarded the packet or not. Pathrater works like a response system. Once Watchdog node decides malicious node in the network, the pathrater works with the routing protocols to avoid the reported node in the future transmission. The dynamic source routing protocol is used in that the routing information is defined at the source node [2]. It might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour report, collision and partial dropping.

K. Balakrishnan et. al. in [19], proposed TWOACK scheme which aims to solve the problem of receiver collision and limited transmission power of Watchdog. TWOACK finds misbe- having links by giving reply to every data packet sent over each three consecutive nodes between the route from the source to the destination. On receiving a packet, each node along the path is needed to send back an reply packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing.

K. Liu et al. in[20], proposed 2ACK scheme serves as an additional technique for routing schemes to find routing misbehavior and to mitigate their adverse effect. The basic idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to do reduction in additional routing overhead, only a part of the received data packets are acknowledged in the 2ACK scheme. The 2ACK scheme tries to find those misbehaving nodes which were ready to forward data packets for the source node but denies to do so when data packets received.

 

Al-Roubaiey et al. in [21], proposed a AACK is a network layer acknowledgement based scheme. It finds misbehaving node instead of misbehaving link and an end to end acknowl- edgment based scheme, to decrease the routing overhead of TWOACK. The AACK scheme may not work well on long paths that will need a significant time for the end to end ac- knowledgments. This limitation will lead the misbehaving nodes more time for dropping more packets. AACK still faces the problem of the partial dropping attacks and false mis- behaviour report.

N. Kang et al. in [22], proposed Enhanced Adaptive Acknowledgment scheme which consist of three parts Acknowledgment, Secure- Acknowledgment, misbehaviour report authenti- cation. This scheme is able to find malicious nodes in the presence of false misbehaviour report.

Elhadi M. Shakshuki et al. in [23], proposed EAACK scheme with digital signature to prevent the attacker from forging acknowledgment packets. All acknowledgment packets mentioned in this research are needed to be digitally signed by its sender and veri_ed by its receiver, due to that it causes the network overhead.

Durgesh Wadbude and Vineet Richariya in [24], proposed secure Ad hoc On Demand Distance Vector Routing (AODV) a novel algorithm for the functioning of such ad hoc networks. Every Mobile node operates as a specialized router and routes are obtained on demand.

## III. METHODOLOGY

### EAACK System in MANET

In Mobile Ad hoc Network (MANET) all nodes are moving within range. Because of wireless network data packets need to be transmitted securely over the network. When data packets are sent to a particular destination it requires the confirmation, that packet has been reached successfully at the destination. But here intruders are those, can lost the data packets in between, for this Intrusion Detection System is required to detect the misbehaving node. The new Enhanced EAACK is designed to deal with three of six weaknesses of watchdog scheme, particularly, false misbehavior, limited transmission power, and receiver collision. The previous approaches of intrusion detection system are failed to detect the false misbehavior, solution to this MRA (Misbehaving Report Authenticate) is introduced. In MRA scheme the send packet ID is checked at the destination is available or not, for this another route has been taken by the DSR (Dynamic Source Routing). Because of this MRA scheme the false misbehavior report is authenticated.

### Proposed Approach

The open medium, dynamically changing topology, lack of central monitoring and management, cooperative algorithms, no clear defense mechanism and wide distribution of nodes makes MANET vulnerable to malicious attacks. Due to the remote distribution of typical MANETs, attackers can simply capture and compromise one or two nodes to achieve this false misbehavior report attack. So, it demands for more secure intrusion detection system. The novel IDS EAACK solves three problems of previous IDS namely, limited transmission power, receiver collision and false misbehavior report. It has three major parts ACK, S-ACK, and MRA. The proposed work evaluates EAACK using DSR and concept of trust in MANET. Trust value of node is reduced based on its behavior in network. In further transmission the node with less trust value is eliminated, which results in increased packet delivery ratio of the system.

| | | | | |
|---|---|---|---|---|
| Data | ACK | S-ACK | MRA | TRUST TABLE UPDATION |

Figure 1: EAACK components

### Architecture

The architecture is given in Figure 2. What should be its input material, how does it process and what is its desired output. Number of nodes and packets are given as input. Then, packets are sends from source to destination across the multiple routes. These are then processed to find out malicious nodes in network. By using DSR routing protocol having route discovery and route maintenance procedure that help to find out new route on demand basis if malicious node is detecting in existing route. And according to that output is gained.

### Algorithm for Proposed EAACK System

Require: mobile nodes Val(nn), Source Node, Destination Node, Packet size,Routing packets from source to destination Create a list Val (nn) A set contains all the information about nodes The source node broadcasts a RREQ packet to find a route to the destination across node.
if RREQ seq. No <= Corresponding RREQ Seq. No
then RREP packets send back to source node
Rebroadcast the RREQ packet across node
end if
if RREP received from all nodes then
Source updates routing information
else
Send RERR Packet if error occurs
end if
Send packet to Destination
if Received ACK packet then

 

Reached packet at destination successfully
else
Switch to S-ACK packet mode
end if
if get Misbehavior Report then
Switch to MRA packet mode
else
Send ACK Packet to Source node
end if
if Send Packet ID== Received Packet ID then
Mark Reporter as Malicious
else
Trust the Report
end if
Send ACK Packet to Source node
Calculate Packet Delivery Ratio (PDR) and Routing overhead.
End

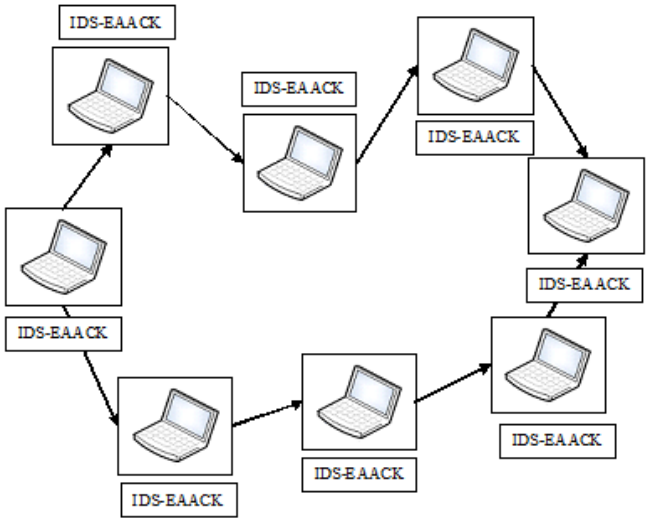

Figure 2: Architecture of the System

**Mathematical Model:**

Let System be S = (I, O, F) Where,

A) I: Set of Inputs (Data Set)

1. Input to system will be a nodes , Source, Destination
2.Set of all possible paths from Source to destination.

RN is the set of all nodes within the route from a source to destination RN = {rn1, rn2, rn3, …}

B) O: Set of Outputs (Result Set)

1. Output will be the node which is misbehaving.
2. Graph representing Packet delivery ratio, Routing overhead, Throughput of the proposed scheme.

C) F: Set of Functions

Let function F be Fn= Fn1, Fn2....Fnn performed on the input to transform it into desired output.

F = {Fn1, Fn2, Fn3} Where,

1. Fn1 = {s1,s2,s3} Where,
   a. s1 = {i|i is to get route from repository for particular destination}
   b. s2 = {j|j is to create a data packet}
   c. s3 = {k|k is to send packet to destination along the route}
2. Fn2 = {s1,s2} Where,
   a.s1 = {i|i is procedure in waiting state till the waiting time is reached}
   b. s2 = {j|j is acknowledgements from intermediate nodes along route}
3. Fn3 = {s1,s2,s3,s4} Where,
   a. s1 = {i|i is process to activate node verification service}
   b. s2 = {j|j is collect verification unicast messages}
   c. s3 = {k|k is to analyze the received verification results}
   d. s4 = {l|l is to broadcast drop node message to all verified nodes}
4. Fn4 = {s1,s2} Where,
   a.s1={i|i is to reduce trust value of drop node}
   b. s2={j|j is to update the path in route cache}

 

## IV. IMPLEMENTATION

**Experimental Setup:**

The proposed trust based EAACK is simulated within Network Simulator (NS2) 2.35 and cygwin environment. TCL and AWK script has been used for implementation. The software is compatible with windows7.

## V. RESULTS AND DISCUSSION

The simulation results here are observed with respect to performance evaluation factors. These performance evaluation factors also contribute to study and analyze the routing misbehavior of the in MANET. The factors which are considered for performance evaluation are given below:

1. Packet Delivery Ratio:- Packet delivery ratio (PDR) defines the efficiency of the network and hence signifies the efficiency of the routing protocol used. The Packet delivery ratio (PDR) is computed as the ratio of number of Received Packets to number of sent packets.
2. Routing Overhead:- Routing Overhead (RO) de_nes the ratio of the amount of routing- related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, MRA, trust table updation].
3. Packet Dropped:- This is the difference between total number of packet transmitted by transmitter and total number of packet received by receiver at receiver end.
4. Throughput: - This is the average number of bits arrived per second at destination node. The metric is used as a measure of the reliability of the protocol under different conditions, hence the average throughput in the network needs to be higher as much as possible. It is the number of packets transferred from one node to another.

In each f the performance parameter the proposed system yeilds better result than the existing one.

## VI. CONCLUSIONS

The self-configuring ability of nodes in MANET made it popular among mission critical applications. The open medium and wide distribution of nodes made MANET vulnerable to malicious attacks. It demand for more secure intrusion detection system. EAACK enhanced using the concept of trust which results in improved performance of the system in terms of increased packet delivery ratio and reduced network overhead. The Trust based EAACK system also solved the limitations of receiver collision, limited transmission power and false misbehavior report of earlier system as well worked on the packet dropping issue of the system.

In future, testing the performance of Trust based EAACK system in real network environment instead of software simulation.

## REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami, "EAACK—A secure intrusion detection system for MANETs",IEEE Transaction on Industrial Electronics, Vol.60,No.3,March 2013, pg no.1089-1098.

[2] Ahmed Sherif , Maha Elsabrouty and Amin Shoukry, "A Novel Taxonomy of Black-hole Attack Detection Techniques in Mobile Ad-Hoc Network (MANET)," 16th IEEE International Conference on Computational Science and Engineering, 2013.

[3] D.Anil and Dr. S. Vasundra , "A Novel Key Exchange Mechanism for Secure Intrusion Detection System for MANET," Journal of Computer Science and Information Technologies, vol. 5, no. 6,pp no. 7126-7129, 2014

[4] Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami,"Detecting misbehaving nodes in MANETs, 12th International Conference on Information Integration and Web-based Applications \& Services, ACM, 2010.

[5] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, vol. 13, no.6, 1999.

[6] Ashish Bagwari, Raman Jee, Pankaj Joshi and Sourabh Bisht, "Performance of AODV Routing Protocol with increasing the MANET Nodes and it's effects on QoS of Mobile Ad hoc Networks," International Conference on Communication Systems and Network Technologies,2012.

[7] Prachee N. Patil and Ashish T. Bhole, "Black hole attack prevention in mobile Ad Hoc networks using route caching", 10thIEEE International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-6, July 2013.

[8] Satveer Kaur and Jagpal Singh Ubhi, "A Simplified Approach to Analyze Routing Protocols in Dynamic MANET Environment," International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 5, Issue-1, March 2015

[9] Qutaiba Razouqi, Ahmed Boushehri, Mohamed Gaballah and Lina Alsaleh, "Extensive Simulation Performance Analysis for DSDV, DSR and AODV MANET Routing Protocols," 27th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2013.

[10] Aarti and Dr. S. S. Tyagi, " Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[11] D. Djenouri, L. Khelladi and A.N. Badache. "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks", Communications Surveys \& Tutorials IEEE, Vol. 7, Issue 4, pp no. 2-28, 2005.

[12] Yuvraj Singh and Sanjay Kumar Jena, "Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad hoc Networks", International Conference on Parallel, Distributed Computing technologies and Applications (PDCTA-2011), Vol. 203 CCIS,2011.

[13] Ashish T. Bhole and Archana I Patil, "Intrusion Detection with Hidden Markov Model and WEKA Tool", International Journal of Computer Applications (IJCA), Vol. 85, No. 13, pp. 27-30, Jan 2014.

 

[14] 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
[15] 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.
[16] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Network", Proc. MobiHoc, June 2002.
[17] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265, ACM 2000.
[18] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network", IEEE International Conference on Communications (ICC'07), pp. 1154-1159, Jun 24-28, 2007.
[19] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.
[20] K. Liu, J.Deng, P. K. Varshney and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs", IEEE Transactions on Mobile Computing, Vol. 6, No. 5, pp. 536-550, May 2007.
[21] Al- Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki and H. Mouftah, "AACK-Adaptive Acknowledge Intrusion Detection for MANET with Node Detection Enhancement", 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp. 634-640, 2010.
[22] N Kang, Nan, Elhadi M. Shakshuki, and Tarek R. Sheltami,"Detecting misbehaving nodes in MANETs", 12th International Conference on Information Integration and Web-based Applications \& Services, pp. 216-222, ACM, 2010.
[23] Nan Kang, Elhadi M. Shakshuki and Tarek R. Sheltami, " EAACK -A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, pp. 1089-1098, March 2013.
[24] DurgeshWadbude and VineetRichariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, Issue 4, pp. 274-279. April 2012.
[25] Sarika Patil and Deepali Borade, "Dynamic Cluster Based Intrusion Detection Architecture to Detect Routing Protocol Attacks in MANET",Sensor Networks and Data Communications(SNDC), Vol. 3, Issue 1, 2014.
[26] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. J. Multimedia System, vol. 15, no. 5, pp. 273–282, 2009.
[27] Sevil Sen, John A. Clark, and Juan E. Tapiador, "Power-Aware Intrusion Detection in Mobile Ad Hoc Networks".
[28] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure routing and intrusion detection in ad hoc networks," in Proc. 3rd Int. Conf. Pervasive Comput. Communication, 2005, pp. 191–199.

 