Security Enhanced Adaptive Acknowledgment Intrusion Detection System

Pawar P.S.
M.G.M.'s College of Engg.,Nanded

Hashmi S.A.
M.G.M.'s College of Engg., Nanded

ABSTRACT
Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. MANET is a collection of wireless mobile nodes forming a network without using any existing infrastructure. In recent years, the use of mobile ad hoc network has been widespread in many applications, security has a most important service in Mobile ad hoc Network compared to other networks. The open medium and wide distributions of nodes responsible for various types of malicious attacks. The solutions for traditional networks are usually not sufficient to provide efficient Ad-hoc operations. This paper proposes and implements a new intrusion detection system named Cryptography Enhanced Adaptive Acknowledgment (CEAACK) specially designed for MANET and compares all existing approaches. And enhancing security level of MANETs based on security attributes the various algorithms, namely RSA and DSA also introduced. The results will be positive performances of WATCHDOG, TWOACK and AACK in the cases of receiver collision, limited transmission power and false misbehavior report.

General Terms
Intrusion Detection System (IDSs), Digital Signature ,Digital Signature Algorithm(DSA).

Keywords
Mobile Ad Hoc NETworks (MANETs), Intrusion Detection System (IDSs),Digital Signature ,digital signature algorithm(DSA),Cryptography Enhanced Adaptive ACKnowledgment (CEAACK).

1. INTRODUCTION
The migration from wired network to wireless network has been a worldwide trend in the past few decades. Due to their natural mobility and scalability wireless networks are always preferred since the first day of their invention. Among all the existing wireless networks, Mobile Ad Hoc NETwork (MANET) is one of the most important & unique applications. Mobile Ad Hoc NETwork is a collection of mobile nodes equipped with both a transmission and receiver that communicate with each other via bidirectional wireless links. One of the major advantages of wireless network is its ability to allow data communication between different parties while maintaining their mobility. But this communication is limited to range of transmitters as shown in Figure 1. MANET solves this problem by allowing intermediate parties to send data transmissions. The MANET is categorized into two types of networks, single-hop network and multi-hop network. In single-hop network, all nodes within the same radio range communicate directly with each other. In multi-hop network [1], nodes depend on other intermediate nodes to transmit if the destination node is out of their radio range .MANET does not require a fixed infrastructure all nodes are free to move randomly [6]. MANET is capable of creating a self-configured & self maintaining network without the help of centralized infrastructure. Due to these characteristics MANET is becoming more popular among industries and critical mission applications.

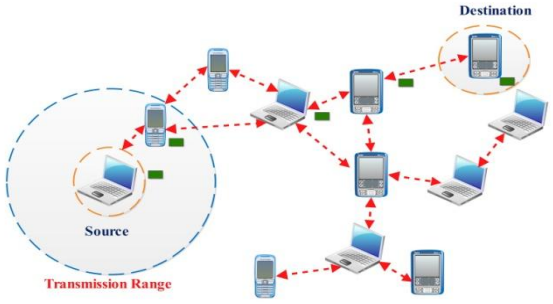


Fig. 1: .Mobile Ad-hoc NETwork

Unfortunately, the open medium & remote distribution of MANET make it vulnerable to various types of attacks. Considering the fact that most routing protocols assume that every node in the network behaves cooperatively with other nodes & is not malicious [1], attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. In such case it is important to develop an IDS specially designed for MANETs. Many research efforts have been devoted to such research topic [2]-[5].

2. EXISTING SYSTEM
This section mainly describes four existing approaches namely, Watchdog [12], TWOACK [10], AACK (Adaptive Acknowledgement) [16] and EAACK [18].

2.1 Basic Watchdog IDS
Marti et al. [12] proposed a scheme called Watchdog. The Watchdog scheme is consisted of two parts namely, Watchdog and Pathrater. Watchdog acts as an IDS for MANETs. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by listening to its next hop's transmission. If the next node does not forward the packet, then it is malicious. The pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets. Watchdog detects malicious misbehaviors by listening to its next hop's transmission. The node's failure counter increases if watchdog node overhears the next node and fails to forward the packet within a specific period of time. Whenever a node's failure counter exceeds a predefined threshold, the watchdog node reports it as misbehaving. The watchdog technique [13],[14] has advantages and weaknesses. The watchdog has the advantage that it can detect misbehavior at the forwarding level and not just link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions 3) limited transmission power,4) false misbehavior ,5) collision 6) partial dropping.

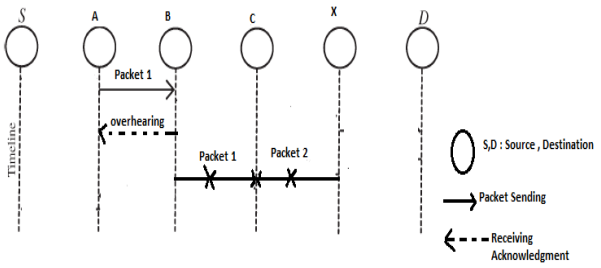


Fig.2: Receiver collisions: At the same time both nodes B and X are trying to send Packet 1 and Packet 2 to node C, respectively.

In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it. This is illustrated in Figure 2.If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives it. Thus, B could skip retransmitting the packet so it is malicious.

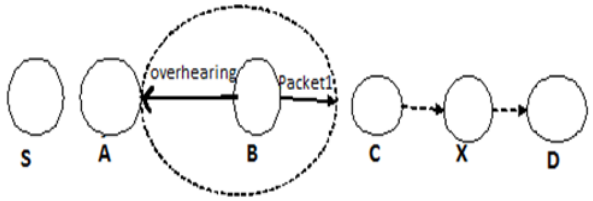


Fig. 3: Limited Transmission Power: Node B limits its transmission power so that the packet transmission can be overheard by Node A but too weak to reach Node C.

In limited transmission power, a misbehaving node can control its transmission power. A misbehaving node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by true recipient (see Figure 3). Only a node with malicious intend would behave in this manner.

In false misbehavior report, as shown in Figure 4, a problem can occur when node falsely report other nodes as misbehaving. For example, node A could report that node B is not forwarding packets when in fact it is. This will cause S to mark B as misbehaving when A is culprit**.**

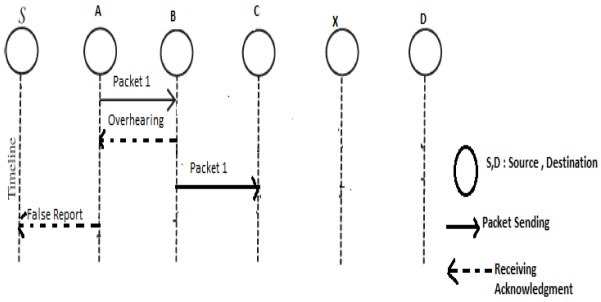


Fig 4. False Misbehavior Report: Node A sends back misbehavior report even though Node B forwarded packet to Node C.

2.2 Two Acknowledgment IDS (TWO-ACK)

TWOACK proposed by Liu et al. [11] is one of the most important approaches among them. TWOACK is neither an enhancement nor a watchdog based scheme. The working process of TWOACK is shown in Figure 5.

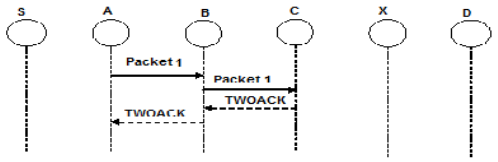


Fig 5 TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops away from it.

Node A first forwards packet 1 to node B. Node B forwards packet 1 to node C. When node C receives packet 1 as it is two hop away from node A, node C must generate a TWOACK packet, which contains reverse route from node A to node C and sends it back to node A .When node A receives a TWOACK packet, it indicates that the transmission of packet 1 from node A to C is successful. Otherwise, both nodes B and C are reported as malicious. The same process is repeated to every three consecutive nodes along the remaining route. This acknowledgment process added a greater amount of unwanted network overhead. And can easily degrade the lifespan of entire network because of battery power consumption.

2.3 Adaptive Acknowledgment (AACK) IDS

Based on TWOACK, Sheltami et al. [16] proposed a new scheme called AACK. The AACK can be treated as a combination of TWOACK and ACK (an end-to-end acknowledgment).The ACK scheme is shown in Figure 6.

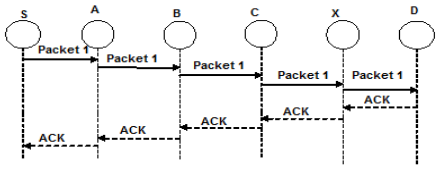


Fig 6 End-to-end ACK IDS scheme: The destination node is required to send acknowledgment packets to the source node.

The source node S sends packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives this packet, it is necessary to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. If the source node S receives this ACK packet within a predefined time, the transmission is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out TWOACK packet. This concept of adopting hybrid scheme in AACK greatly reduces the network overhead. TWOACK and AACK overcome the three weaknesses of Watchdog, namely, receiver collision and limited transmission power. But both of

these still fail to detect malicious nodes which sends false misbehavior report & forged acknowledgment packets.

The goal is to propose a new IDS modeled for MANETs which solves not only receiver collision and limited transmission power but also false misbehavior problem. Moreover, extend the model to adopt a digital signature scheme while transmitting the packets. Because in all acknowledgment based IDS, it is important to ensure the integrity & authenticity of all acknowledgment packets.

2.4 Enhanced Adaptive Acknowledgment (EAACK) IDS

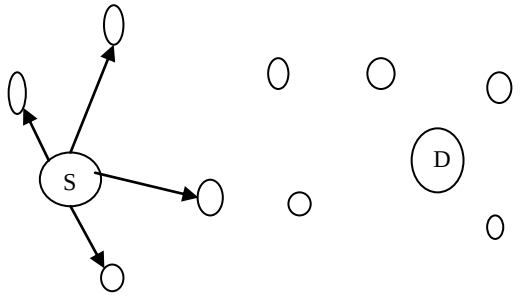
EAACK is based on both DSA [17] and RSA [15] algorithm. The three parts of EAACK system are ACK, secure ACK(S-ACK) and Misbehavior Report Authentication (MRA).EAACK is also an acknowledgment based IDS. This scheme uses the digital signature method to prevent the attacker from forging acknowledgment packets. Before the acknowledgment packets sent out EAACK requires the whole acknowledgment packets are digitally signed and verified by its receiver until they are accepted.

3. PROPOSED SYSTEM

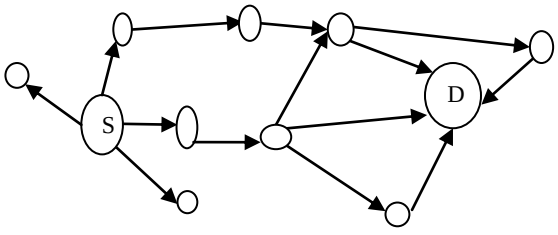
This section discusses proposed model which is composed of four major modules.

3.1 Basic Routing Module

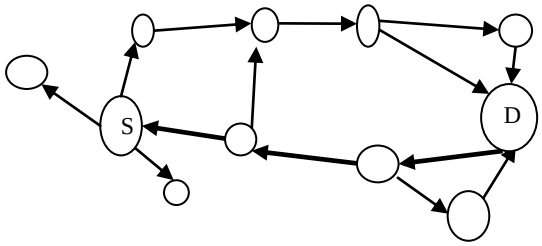
It is an on-demand, source routing module. If the source has no path to destination, then source initiates a route discovery in on-demand fashion. Figure 7 demonstrates the process. Node S (source) wants to communicate with node D (destination) but does not know any paths to D. S starts a route discovery by broadcasting a route request packet to its neighbors that contains the destination address D(see Figure 7(a)). This process continues until a route request packet reaches to destination D (see Figure 7(b)). The node D now send route reply packet to inform S about the discovered route (see Figure 7(c)).



(a) Node S sends route request packet to find a path to node D.



(b) The route request is forwarded throughout the network.



(c) D sends a route reply to S .The thick lines represents the path chosen to send route reply packet to source node.

Fig.7 Example of basic routing.

3.2 Acknowledgment Module

This module is basically end-to-end acknowledgment scheme. Its task is to reduce network overhead when there is no network misbehavior is detected. In this mode, the source node sends ACK data packet to destination node. When the packet reaches at destination, the destination node requires to send ACK packet back to source node. If in a particular time the source node receives the ACK packet, the data transmission is successful. Otherwise, source node will change to S-ACK mode by sending S-ACK data packet to detect misbehavior nodes.

3.3 Secure Acknowledgment(S-ACK) Module

In this scheme every three successive nodes works in a group. In the three successive nodes the secure acknowledgment packet is sent by third node to first node. The S-ACK scheme can detect malicious nodes if there is receiver collision or limited transmission power. If secure acknowledgment not received it means it will report those nodes as misbehaving nodes to the source node [8]. But the source node will switch to Misbehavior Report Authentication (MRA) module to **ensure the correctness of received report.**

3.4 Misbehavior Report Authentication Module (MRA)

Normal nodes can be reported as malicious because of false report information. To solve this problem, the MRA scheme is introduced to authenticate whether the destination node has received the reported missing packet through different route. At the beginning the source node finds its local knowledge base and identifies the other route to the destination node. If there is no route to destination then source node search other route by DSR routing request [7]. When the packet received at destination, it compares whether the reported packet was received or not by using local knowledge base. If it is received

then it is decided that a report is false misbehavior report. And the reported node is malicious one.

4. SIMULATION CONFIGURATION AND SYSTEM RUN

Simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform Ubuntu 10.04. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM. In NS 2.34, configuration specifies 30 nodes in a flat space with a size of 670 × 670 m. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2. The moving speed of mobile node is limited to 20 m/s User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 512 B. The packets are

routed using Ad Hoc On-demand distance vector routing protocol and the acknowledgment packets are authenticated using RSA [15] and DSA [17] algorithm.

The proposed model is tested with other intrusion detection system in many scenarios which includes:

1) BAODV: Basic Ad-hoc On Demand Vector scenario.
2) BAODV_M: Basic Ad-hoc On Demand Vector with malicious node scenario.
3) TWO-ACK: Two Acknowledgment ID scenario.
4) AACK_M: Adaptive Acknowledgment ID with malicious node scenario.
5) AACK_FM: Adaptive Acknowledgment ID with Fake Acknowledgment malicious node scenario.
6) EAACK_M: Enhanced Adaptive Acknowledgment ID with malicious node scenario.
7) CEAACK: Cryptography Enhanced Adaptive Acknowledgment ID scenario.

And for each scenario, the value of performance metrics [9] Packet Delivery Factor (PDF), Routing Overhead (ROV) is estimated to evaluate performance of IDS for existing and proposed technique.

BAODV:

Data transmission from source to destination is done without any security. Initially, the source node 0 broadcast route request packet to its neighbors in the search of destination node 35. As shown in Figure 8. If this packet reaches to destination, the destination node sends route reply packet to source which is illustrated in Figure 9. If there is any malicious node found in the path means node cannot detect malicious node information.

BAODV_M: In Basic Ad-hoc On Demand Vector with malicious node scenario when malicious node appears the Packet Delivery Factor (PDF) drop.

In TWO-ACK scheme [10], while transferring the data each node need to generate the acknowledgment ACK after receiving the data and that should be forwarded to previous node. And at the same time each node has to forward the ACK of next node to previous node. By this method one can find the intermediate malicious node. But this method increases the network load while sharing the number of acknowledgment.

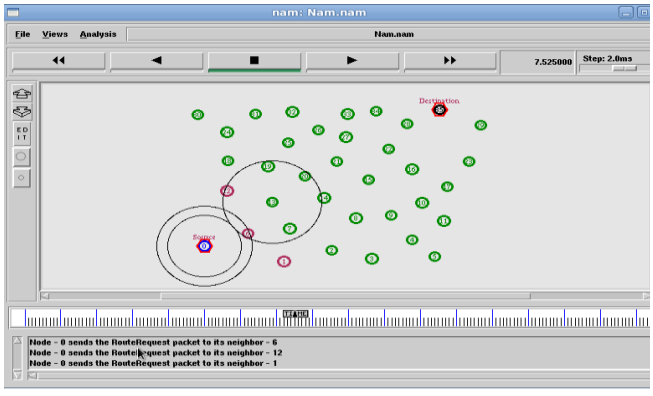


Fig. 8 Source node sends route request packet to its neighbors.

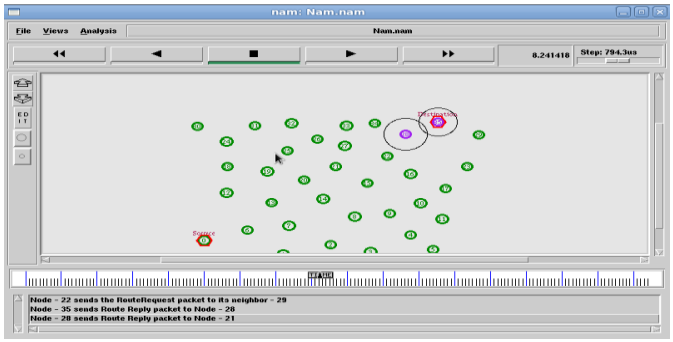


Fig. 9 Destination node sends route reply packet to source.

When AACK method is used, it can provide same security as well as reduced overhead. In this scheme before attack end-to-end Acknowledgment ACK used to reduce the overhead and while attack the source node will switching to TWO-ACK model mode to find the malicious node.

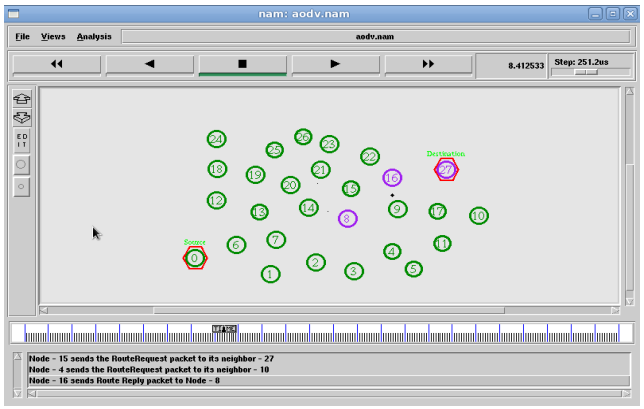


Fig.10 Node drops all packets that they receive

This scenario simulated a basic dropping attack. Malicious node just drop all the packets that they receive, as shown in Figure 10.InEAACK_M Enhanced Adaptive Acknowledgment ID with malicious node scenario, malicious node collects the data but there is no ACK to source node .The malicious node can't generate the ACK so by that source can find attack, and source will switch to Secure ACK(S-ACK) mode to find the malicious node. By this method one can find malicious, as shown in Figure 11.

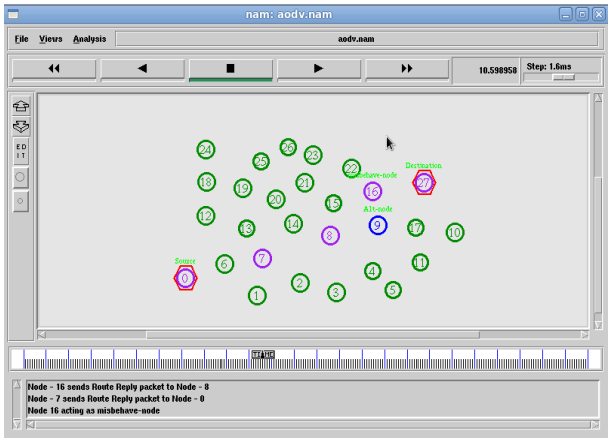


Fig.11. Node is detected as malicious

After detection of malicious node, the EAACK_M scheme

should avoid this node and select the alternative node to send packets in future. The alternative node could be the one which is next nearest node to destination node which is illustrated in Figure 12.

EAACK_M requires all acknowledgment packets to de digitally signed using RSA algorithm before they are sent out and verified until they are accepted. In RSA algorithm, public key and private key used to share the message. The key are denoted as public key (e, N) and private key (d, N). To generate keys we have to use two prime numbers by key generation. To make encryption the nodes should share the public key (e, N) to all other node. By using public key (e, N) value, the hacker can find private key (d, N) by using RSA algorithm. The encrypted message is sent to destination, as shown in Figure 13.

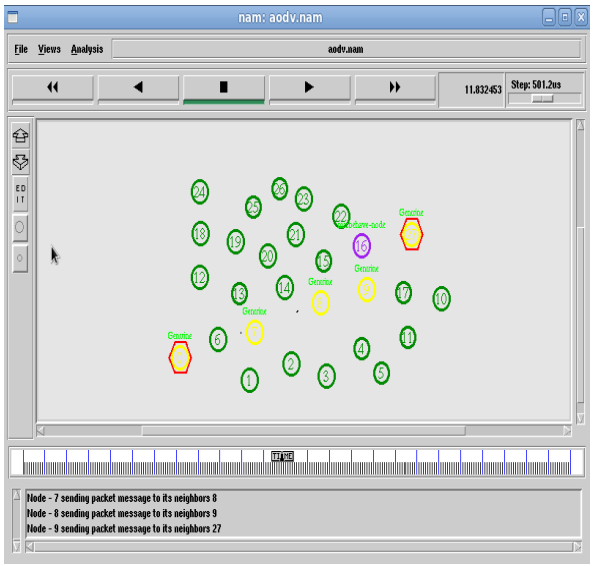


Fig. 12 Alternative node selected to send the packets further

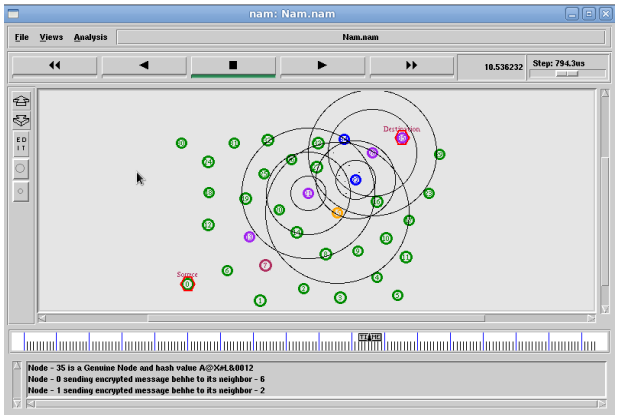


Fig. 13 Source node sends encrypted message to destination.

To solve the problem of forged acknowledgment attacks, the proposed model Cryptography Enhanced Adaptive Acknowledgment (CEAACK) ID scenario with cryptography technique is run. Including hybrid Cryptography in CEAACK to prevent the attackers from initiating forged acknowledgment packets are encrypted and digitally signed by using DSA and RSA algorithm before they are sent out and verified until they are accepted.

5. PERFORMANCE EVALUATION OF PROPOSED MODEL

In order to provide a better vision on simulation results, the following two performance equations evaluate the performance of IDS for existing and proposed technique and are defined as follows:

5.1 Packet Delivery Factor (PDF)

It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source. Figure 14 shows the results based on PDF.

$$PDF = \frac{\sum Received\ packet\ at\ destination}{\sum Sent\ packet\ by\ source}$$

5.2 Routing Overhead (ROV)

It is the ratio of routing related packets in bytes (RREQ, RREP, RERR, and AACK) to the total routing and data transmissions (sent or forwarded packets) in bytes. It means that the acknowledgments, switching over head are included. Figure 15 shows the results based on ROV.

$$OV = \frac{\sum Routing\ \ transmissions}{\sum Data\ \ transmissions\ \ + \sum Routing\ \ transmissions}$$

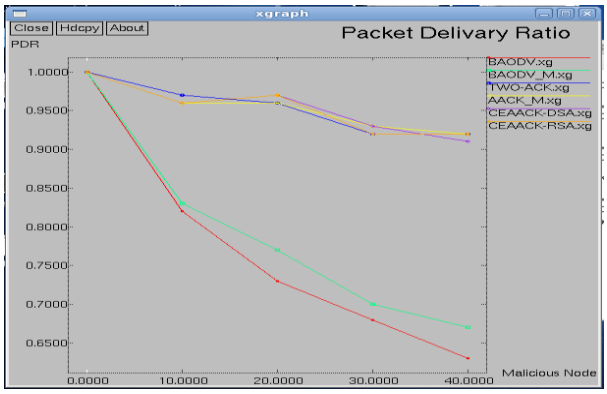


Fig. 14 Comparison of Packet Delivery Factor (PDF)

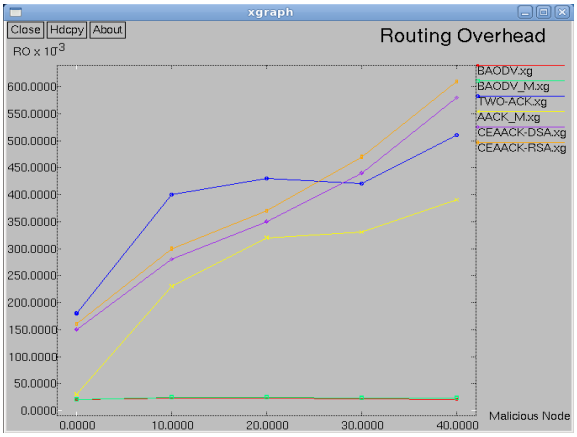


Fig. 15 Comparison of routing overhead

6. CONCLUSION

This paper analyse the effects of routing misbehaviour in ad hoc networks. The security in the mobile Ad-hoc networks provided by implementing a new intrusion-detection system named Cryptography Enhanced Adaptive Acknowledgment (CEAACK). In the CEAACK all acknowledgment packets are encrypted and digitally signed before they are sent out and verified until they are accepted. The proposed Model

completely overcomes the weaknesses like receiver collision, false misbehavior, and limited transmission power. All acknowledgment packets in the model are authentic. The proposed model can significantly improve the Packet Delivery Factor (PDF).

To increase the merits of research work; future plan is to investigate the following issues in the research:

1) Examine the possibilities of adopting a key exchange mechanism that does not require any Trusted Third Party for key management to eliminate the requirement of pre distributed keys.

2) Performance of proposed model (CEAACK) is to be tested in real network environment instead of software simulation.

7. REFERENCES

[1] Buttyan, L. and Hubaux, J .P .2007.Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press.

[2] Dondi,D., Bertacchini,A.,Brunelli, D. ,Larcher,L., and Benini,L.2008.Modelling and optimization of a solar energy harvester system for self-powered wireless sensor networks. IEEE Trans. Ind. Electron., vol. 55, no. 7, pp.2759–2766.

[3] Gungor,V. C. And Hancke, G. P. 2009.Industrial wireless sensor networks: Challenges, design principles, and technical approach. IEEE Trans. Ind. Electron., vol. 56, no. 10.pp.4258–4265.

[4] Hu,Y.,Johnson, D., and Perrig,A. 2002.SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks.In Proc. 4th IEEE Workshop Mobile Computer Syst. Appl. pp3–13.

[5] Hu,Y., Perrig,A., and Johnson,D.2000.ARIADNE: A secure on-demand routing protocol for ad hoc networks. In Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA. Pp.12–23.

[6] Jayakumar,G. And Gopinath,G. 2007.Ad hoc mobile wireless networks routing protocol—A review. J. Comput. Sci., vol. 3, no. 8.pp.574–582.

[7] Johnson,D. And Maltz,D. Dynamic Source Routing in ad hoc wireless .pp.153–181

[8] Kang,N., Shakshuki ,E., and Sheltami,T.2010 .Detecting misbehaving nodes in MANETs. In Proc. 12th Int. Conf. iiWAS, Paris, France. pp.216-222.

[9] Kang,N.,Shakshuki,E., and Sheltami,T.2011.Detecting forged acknowledge in MANETs. In Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore.pp. 488–494.

[10] Lee,J.S., 2008.A Petri net design of command filters for semiautonomous mobile sensor networks. IEEE Trans. Ind. Electron., vol. 55, no. 4.pp.1835–1841.

[11] Liu,K.,Deng,J.,Varshney,P.K. and Balakrishnan,K.,2007. An acknowledgment-based approach for the detection of routing misbehaviour in MANETs. IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550.

[12] Marti,S., Giuli,T.J., Lai,K., and Baker,M. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In Proc. 6th Annu. Int. Conf. Mobile Computer Network, Boston, MA, pp. 255-265.

[13] Parker,J., Undercoffer,J., Pinkston,J., and Joshi,A.2004 .On intrusion detection and response for mobile ad hoc networks.In Proc. IEEE Int. Conf. Perform., Comput., Commun., pp. 747–752.

[14] Patcha,A., and Mishra,A.2003.Collaborative security architecture for black hole attack prevention in mobile ad hoc networks.In Proc. Radio Wireless Conf., pp. 75–78.

[15] Rivest,R.,Shamir,A., and Adleman,L.1983 .A method for obtaining digital signatures and public-key cryptosystems.Commun. ACM, vol. 21, no. 2, pp. 120–126.

[16] Sheltami,T., Al-Roubaiey,A., Shakshuki,E. and Mahmoud,A.,2009.Video transmission enhancement in presence of misbehaving nodes in MANETs. Int. J.Multimedia Syst.,vol. 15, no. 5, pp. 273-282.

[17] Nat. Inst. Std. Technol., 2009. Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, Digital Signature Std.

[18] Shakshuki,E.M.,Kang,N.andSheltami,T.R.2013 EAACK A Secure Intrusion-Detection System for MANETs.In IEEE Transactions on Industrial Electronics, vol. 60, no.3.