International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Intelligent Enhanced Adaptive ACKonwledgement model for security of MANETs

Chetan S Kadu†* and Ganesh K Pakle†

†Department of Information Technology, Shri Guru Gobind Singhji Institute of Engineering and Technology [Autonomous], Vishnupuri Nanded, Maharashtra, India

Accepted 05 July 2015, Available online 11 July 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

In Recent year MANET became a favored technology due to their advantages and applications. MANETs is a collection of data terminals equipped with wireless transceivers that can communicate with one another without using any fixed network infrastructure. MANETs is infrastructure less. Single node act as both transmitter and receiver. Both nodes communicate when they are in the same range. Otherwise, they depend on their neighbors to relay messages. Now a days Intrusion detection system plays vital role in the Security of MANETs. IDSs are able to solve various security attacks in MANETs. However, the distributed nature of nodes can cause various malicious attacks on MANETs. In MANETs the dynamic nature of network topology results in frequent path breaks. To addresses potential security issues. In this paper, we propose a new intrusion detection system called Intelligent Enhanced Adaptive ACKnowledgment (IEAACK) specially design for MANETs. The proposed system introduces a global digital signature to prevent the attacker from forging acknowledgment packets. Furthermore, we propose a trust prediction model to secure the network effectively.

Keywords: *Mobile Ad hoc Network (MANET), Digital Signature. (IEAACK) Intelligent Enhanced Adaptive ACKnowledgement*

1. Introduction

By definition of Mobile ad hoc Network (MANET) is a collection of data terminals equipped with wireless transceiver that can communicate with one another without using any fixed network infrastructure. Mobile ad hoc network (MANET) is an infrastructure-less, self-configuring network of mobile nodes connected wireless link either indirectly or directly. MANET used in various industrial applications and security purpose application (Jiazi YI, 2008). Most favored form of wireless network in use today is wireless local area network (WLAN).A WLAN is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area companies, schools, home. Due to limitation of WLAN that it's receiving a fixed infrastructure researcher look forward towards MANET. One of the advantages of MANET is data communication between various mobile nodes by maintaining their mobility. Furthermore, due to limited range problems means two nodes beyond the communication range cannot communicate. MANET overcomes this problem by introducing intermediate nodes to relay data transmission. MANET can be achieved by dividing networks into two type's single hop and multihop. All the nodes which are in the same radio range directly communicating with each other in the single hop network. On the other side nodes depend on the intermediate nodes to transmit if destination node is not available in the radio range in multi hop network. In reverse to traditional wireless network, MANET doesn't required fixed infrastructure, so every node free to move dynamically (G. Jayakumar, *et al,* 2007).

MANET is capable by producing a self-configuring and self-maintaining network without the aid of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Quick deployment and less configuration make MANET favored in emergencies where an infrastructure difficult to establish in several cases such medical emergency situations, conflicts in military (N.Nasser, *et al,* 2007).

As we know MANET can vulnerable by serval type of attacks due to open access and dynamic distribution. In MANETs most of the routing protocol assumed that every node act as cooperatively with other nodes and not suspicious or noncooperative nodes into the network. However MANETs dynamic nature topology and centralized approach of monitoring fails to detect various intrusion in networks, it is not possible to

*Corresponding author: **Chetan S Kadu**

designed IDS which provides all security aspects. We modify the existing system for security of (Elhladi M.Shakshuki, *et al* ,2013).

2. Related work

(Elhladi M. Shakshuki, *et al*, 2013) in this paper authors proposed a novel IDS named as EAACK, over drawback of existing IDS i.e. watchdog, TWOACK and AACK and overcome the problem such as limited transmission power ,ambiguous collision, receiver collision, false misbehavior report. But the main focus is on the false misbehavior report and Forged acknowledgement packet. The advantages over existing systems of this proposed system is detection of higher malicious nodes.

(G. Jayakumaret, *et al*, 2007) in this paper author discuss ad hoc routing protocol which can be divided into two parts demand based and table driven. AS we know routing protocol wired network not in ad hoc network due dynamic nature of nodes. As we know mobile computing is favored technology and keep growing with different integration of MANET with wireless network and static internet infrastructure.

(N. Nasser *et al,* 2007) in this paper authors discuss the limitation of watchdog and to overcome the weaknesses, they proposed the novel Intrusion detection system known as Exwatchdog. The main advantage to design this system is ability to discover malicious nodes. By this system we increase the throughput and decrease the overhead.

(Stephen Mueller, *et al,* 2004) MANET nodes are distinguish by their mobility, limited power, and memory resources. Due to the limited range problem we constantly required intermediated nodes to get communication media to the destination. One of the serious issue in MANET is routing. This paper discus all multipath routing problem.

3. Problem definition

Researchers have proposed a number of collaborative IDS systems.

1) Watchdog
2) TWOAK
3) AACK

1. Watchdog

(Marti, *et al*, 2000) the 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
6) Partial dropping

2. TWOAK

TWOACK proposed by (Liu *et al,* 2007) The main motivation of TWOACK to overcome the weakness of watchdog such as limited transmission and receiver collision also TWOACK detect the misbehaving link by acknowledgment to every transmitted packet via three continuous nodes from source to destination. But in this scheme network overhead present.

3. ACCK

(Sheltami *et al*, 2009) proposed a new scheme known as Adaptive ACK. This scheme combination of TACK and ACK.In this scheme source will switch to TACK, if source doesn't get ACK packet before timeout occur. Both schemes fail to overcome the problem of false misbehavior report and forge acknowledgment packet.

4. Scheme description

4.1 Proposed Architecture

Our proposed architecture divided into 4 sections

1) ACK
2) S-ACK
3) MRA
4) Digital signature

1. ACK

It is basically an end to end acknowledgment scheme. It is a part of EAACK scheme main motto to reduce the network overhead when no network detected. The basic flow is if node A sends a packet p1 to destination D, if all the intermediate nodes are cooperative and successfully receives the request in the node D. It will send an ACK to the source (Node A). If ACK from the destination get delayed then SACK process will initialize.

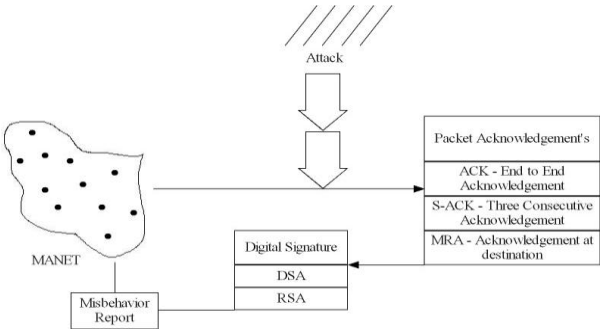

Fig. 1 Intelligent Adaptive ACK trust model

2. S-ACK

In the SACK we consider 3 consecutive node, suppose N1 N2 N3 work in group to detect misbehaving nodes in the network. If Node N1sends out SACK data packet to N2 and it forward to N3, if it is successful

transmission then N3 sends out SACK ack packet to N2 and it will forward to N1.if Node fails to receive this ack packet within timeout period then both Nodes N1 and N2 are marked as malicious. Then source node switch to MRA mode to detect false misbehavior in the transmission.

3. MRA

In MRA scheme source node finds alternative path to reach the destination based on prior knowledge. As we know the MANET capable to finds out multiple path between two nodes. Now if packets reaches destination via the generated path created by source then that packet is declared as the false report

4. Digital Signature

In above all scheme i.e. ACK, SACK, MRA basically we used acknowledgement based detection. All misbehavior in the network is detected by acknowledgement packets. So it is important to that all acknowledgment packets are in IEAACK are authenticated by some digital algorithm. So we used the global key distribution in our proposed method. So that we can control forging acknowledgement. It can prevent the vulnerability from outsider.

4.2 Implementation

To cross check the implementation of IEAACK trust model. We used the network simulator i.e. NS 2.34, and for performance evaluation we used the default configuration which specifies 50 node, simulation area 500×400. Maximum four hops are allowed in this configuration setting. We used network interface type physical and MAC layer model 802.11. Transmission range between 50 to 300.Transmission control protocol with CBR is having packet size 512 B. In order to measure the performance of our proposed scheme, we consider performance metric.

1. Packet Delivery Ratio

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

Number of packet receive / ∑ Number of packet send
The greater value of packet delivery ratio means the better performance of the protocol.

2. Routing Overhead

Routing Overhead is the number of routing packets required for network communication.

1) RREQ (Route request)
2) RREP (Route reply)
3) RERR (Route error)

At the time of simulation source node broadcast the RREQ message to its neighbors within its range of communication. After receiving the RREQ message, neighbor attached their address and broadcast the message to other neighbors. If same request of RREQ message is built more than the ones it simply push aside. If the inactive node found, then RERR message is send to the source node, it generally breaks in the link. If RREQ received by given destination. Then destination node initiates the RREP back to the source prior to knowledge of RREQ message. Now we discuss the digital signature schemes, to compare the performance of DSA and RSA schemes. We generate the 1024-b DSA and RSA key for each node in the network. We used global distribution of key. The following table 1 shows the file size of public private, and signature size in DSA and RSA (Nat. Inst. Std. Technol ,2009),(R. Rivest, *et al*, 1983).

Table 1: File size of keys and signature

Scheme	Private key	Public key	Key	Signature
DSA	509 B	654 B	1024 B	89 B
RSA	916 B	272 B	1024 B	131 B

DSA is faster when generating a key than RSA.RASA on other hand is faster at encryption than DSA, while decrypting, DSA is faster mainly due to is the great decryption capability. If you need digital singing DSA is the encryption algorithm of choice and for verification of digital signature RSA is the best choice.

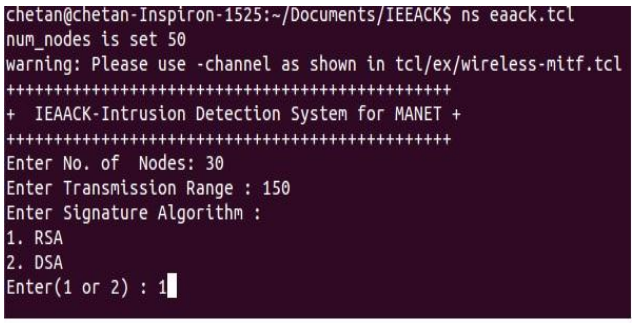

Fig. 2 Input to system

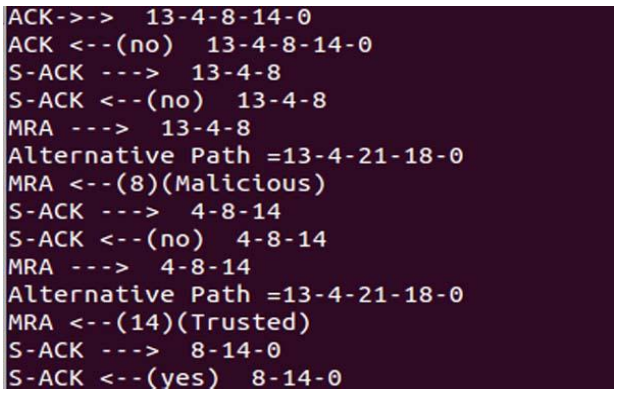

Fig. 3 Acknowledgement action

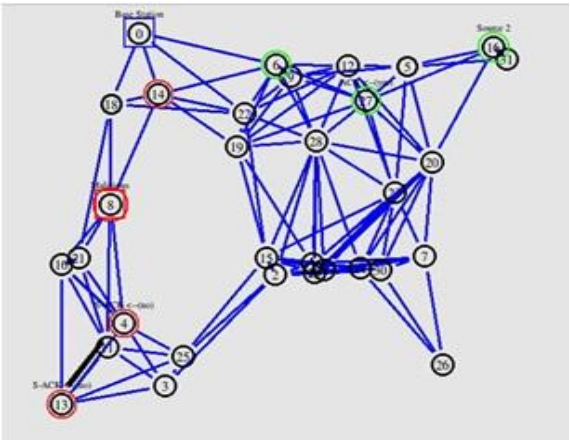

Fig.4 Entire topology after detection

5. Results and discussion

As our simulation result fig 5, fig 6, fig 7 shows the PDR, RO, and performance evaluation of DSA and RSA scheme respectively. Where in all our simulation DSA scheme produces the low measure of overhead comparatively to RSA. It can be realized because the signature size of DSA is less than RSA. Moreover, it is observe that RO is vary as no of malicious node increases. Whit respective to the result we conclude that DSA scheme is more suitable for MANET.

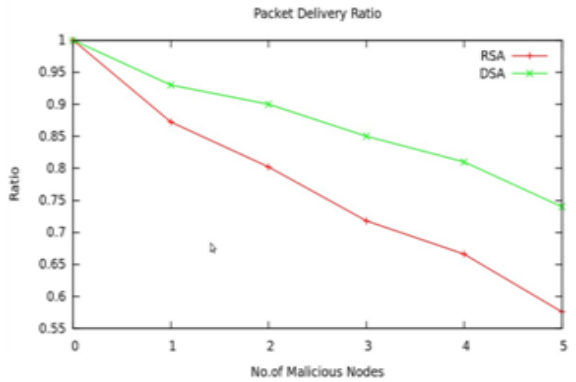

Fig. 4 Packet delivery ratio of DSA and RSA scheme

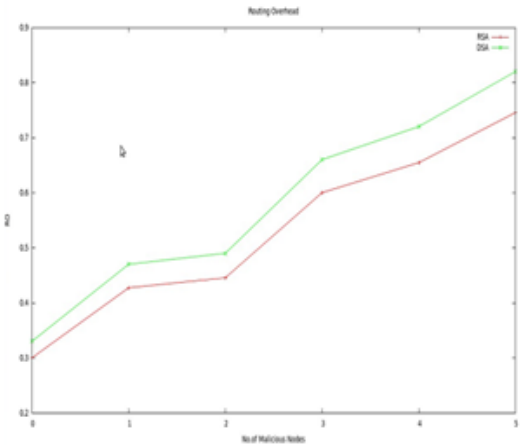

Fig. 5 Routing overhead of DSA and RSA scheme

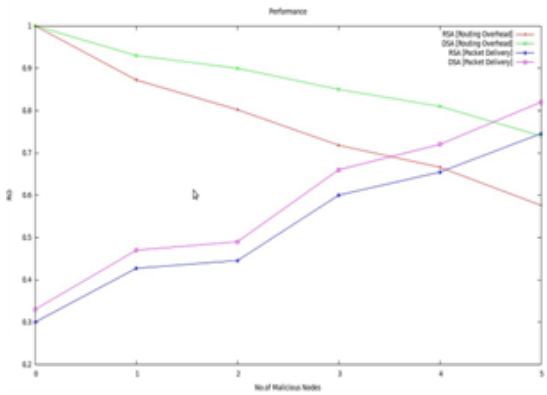

Fig. 6 Performance comparison

Conclusion and future work

One of the security threats in MANET is packet dropping attack. In this paper we come with novel trust model name as IEAACK. In this scheme we compare the digital signature under DSA and RSA scheme. We successfully overcome the weakness of false misbehavior, receiver collision limited transmission. In our proposed trust model we compare the performance using performance metric i.e. PDR and Ro. We implement the both scheme DSA and RSA in our simulation. We used global key distribution concepts where we distribute the key to each node.AS our simulation results conclude that DSA scheme is better for MAENTs.

In future we extend the concept of this scheme using multipath routing approach along with possibilities of hybrid cryptography scheme .We propose a trust prediction model to secure the network effectively. The goal of our system trust worthiness of nodes, based on the historical behaviors of nodes.

References

Elhladi M.Shakshuki, Nan Kangand Tarek R.Sheltami(2013),EAACK—A Secure Intrusion – Detection System for MANETs, in IEEE transactions ONIndustrial Electronics, vol. 60,NO.3.

Jiazi YI, (2008) A Survey on the Applications of MANET Polytech' Nante.

G. Jayakumar and G. Gopinath(2007),Ad hoc mobile wireless networks routing protocol—A review, J. Computer. Sci.,vol. 3, no.8, pp.574–582,

N. Nasser and Y. Chen(2007), Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network,in Proc. IEEE Int Conf. Commun. , Glasgow, Scotland, Jun.24–28,pp. 1154–1159.

Stephen Mueller, RoseP.Tsang, Dipak Ghosal, (2004) Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges Performance Tools and Applications to Networked Systems, Volume 2965, pp 209-234.

Nat. Inst. Std. Technol (2009), Digital Signature Standard (DSS) Federal Information Processing Standards Publcation, Gaithersburg, MD, Digital Signature Standard (DSS).

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

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

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

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