Detection of Routing Misbehaving Links in MANET by Advance EAACK Scheme

Shraddha Kamble[#1], Dr.B.K Mishra[*2], Dr.Rajesh Bansode[#3]

[#1] *PG student, Electronics and Telecommunication Department, Mumbai University*

[*2] *Principal, Electronics and Telecommunication Department, Mumbai University*

[#3] *Associate Professor, Information Technology Department, Mumbai University*

Mumbai, India

Abstract-- *Mobile Ad hoc networks (MANETs) consist of a set of mobile nodes which can move about freely and they use radio frequencies in air to transmit and receive the data. MANETS is used in many critical and tactical operations due to flexibility provided by their dynamic structure. Hence security becomes a primary concern to have safe communication between two nodes and this itself emphasis the need for an efficient intrusion detection system in MANETs. Enhanced Adaptive Acknowledgment (EAACK) was introduced in our earlier research which has overcome the drawback of Watchdog, ACK and TWOACK to some extent. In our paper, we have identified the inadequate nature of EAACK in scenarios of link breakage, source maliciousness Due to continuous and changing nature of nodes MANET nodes contributes to frequent link breakages in the network which leads to path failures and route discovery processes. In order to send the data from one node other broadcast mechanism is used which increase the overhead between two nodes. Hence, in order to increase overall efficiency and security parameters that are considered are routing overhead and throughput.*

Keyword — *Adaptive acknowledgment (AACK), Dynamic source routing (DSR) , Digital Signature Algorithm (DSA),EAACK (Enhanced Adaptive Acknowledgment) ,Misbehaviour Report Analysis (MRA),MANETS (Mobile Ad-hoc Networks) , IDS (Intrusion Detection System)*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) is one of the most widespread areas of research recently because of the challenges of the related protocols. MANET (Mobile Ad-hoc Network) technology which enables users to communicate with each other without any physical infrastructure regardless of their location, that's why it is referred as infrastructure less network. Mobile Ad hoc Network, or MANET, consists of a group of nodes that dynamically constructs a self-configuring network without the support of a centralized network infra-structure. The mobile nodes can be cell-phones, PDAs and laptops and Bluetooth, etc.

Device in mobile ad hoc network should able to detect the presence of other devices and perform necessary set up in order to communicate and share the data. One advantage of wireless networks is they can transmit data even after remaining mobile. Mobile Ad hoc networks makes less saviour, the problem of out of range nodes by routing data through intermediate nodes intermediate acts as a middle man in between two nodes. The MANET[1][2] operates independently and can be connected to the larger Internet. MANETS require less space and quick configuration due to this feature it is mainly used in emergency situation like medical emergency and military application where infrastructure is not available.

Due to these unique characteristics, MANET is becoming more and more widely implemented. Being incorporated in critical operation security is of vital importance . Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. An effective way of incorporating defective nodes in network in implementing intrusion detection system. It act as second layer of security it scans the whole system and detect undesirable and intruder activities .

The remainder of the paper is organized as follows. Section II presents the background review and related work that are important for the understanding of the material to follow. Section III introduces our intrusion detection and EAACK(Enhanced Acknowledgment system). Section IV reports the simulation results and discussion. Finally, conclusions drawn from the paper and future work are given in Section V.

II. BACKGROUND

A. Intrusion detection in MANETs

In Mobile Ad-hoc Network it is always assumed that the each node cooperates with other in order to send the data to each other. This assumption leaves the attackers opportunities to attack the system with just one or two compromised nodes .In order to address this problem Intrusion detection System[3] should be added to improve the security level of MANETs. Intrusion detection have the ability to detect and report the malicious activity in the network so it may be possible to stop that activities before they cause damage to the network . Intrusion in this section, we mainly describe three existing approaches, namely, TWOACK, AACK and EAACK.

B. WATCHDOG

Watchdog is an intrusion detection system that detects the presence of misbehaving nodes in the network. The Watchdog scheme mainly consist of two parts Watchdog and Pathrater [4]. Watchdog is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listening to its next hop's transmission .If watchdog overhear that it fails to transmit the packet within defined amount of time ,it increases failure counter. If the failure counter exceed predefined time the node is misbehaving node. While Pathrater cooperates with routing protocol to avoid reported node in future transmission. Watchdog is more capable in detecting malicious nodes than the malicious link.

Due to the limitation of detecting the node in forwarding level and not on link level makes watchdog scheme fails and hence fails to detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehaviour report, 5) collusion, and 6) partial dropping.

C. TWOACK

TWOACK is neither enhancement nor watchdog based scheme. TWOACK scheme works in three consecutive nodes to detect misbehaving node .When a first node forward a packet the routing agent verifies if the packet is received successfully by the destination that is two hop away from it.The same process applies to all other three consecutive nodes down the route. Otherwise, if this TWOACK packet is not received in a specific time period, other two node are marked as malicious nodes. The TWOACK successfully solves watchdog collision and limited transmission power problems. However, the acknowledgment process required in every packet transmission process added a major amount of unwanted network routing overhead and also considering the limited battery power of MANETS such unneeded process can degrade the overall performance of entire network.

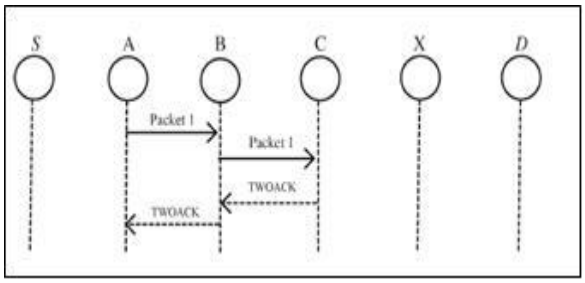

Figure 1 TWOACK SCHEME : Each node is required to send back an acknowledgement that is two hops away from it.

D. AACK

AACK is based on TWOACK Acknowledgement similar to TWOACK, AACK is acknowledgment based network layer scheme and can be considered as a combination of scheme TACK (Identical to TWOACK) and ACK. Compared to TWOACK, AACK significantly reduces network overhead and also capable of maintaining the same throughput. The concept of adapting hybrid technology is to greatly reduce the network overhead. But the problem of both TACK and TWOACK scheme is they fail to detect malicious node in presence of false misbehaviour report and forge acknowledgement packets.

III. EXISTING SYSTEM

A. ACK

As discussed earlier ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehaviour is detected. When source node sends the data packet it also generates packet id and sending time. When data reach to destination node it is required to generate an ACK packet that contain receive packet id and send it back to source node in opposite direction via same route. On the other hand if source node does not receive packet in specific time it switches to S-ACK mode.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK and it works similar to TWOACK scheme only difference is a flag is added to the packet indicating type of packet. Again the source node is required to store the packet ID and sending time. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node from second node. By doing this we can solve the problem of receiver collision or limited transmission power.

Unlike TWOACK scheme , in S-ACK scheme when a misbehaviour node is detected instead of trusting the report marking node as malicious , a misbehaving report is send to source node and source node switches to MRA scheme by sending out MRA packet to destination node through different route.

C. MRA

As discussed earlier when in S-ACK scheme is detected with misbehaving node instead of trusting the report ,the report is send to source node and source node send it to MRA scheme and MRA packet is send to destination through different route. MRA packet contains the ID of the packet that has

been sent out .Dynamic source routing is used to find the new route. When the destination node receive the MRA packet, it searches it local memory to see if there is a match to requested packet id.If it matched then destination node must have received the data packet and whoever reported the misbehaviour is malicious node .On the other side if no match is found then it is safe to conclude that misbehaviour report is valid.

D. Digital Signature

EAACK is an acknowledgment based IDS hence all the three parts of EAACK namely, ACK, S-ACK, and MRA, are also acknowledgment-based detection schemes. Thus they all depend on acknowledgment packets to detect misbehaviours in the network. Thus, it is important to ensure that all acknowledgment packets in EAACK are authentic. Otherwise, if the attackers are smart enough, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to overcome this problem digital signature are introduced . Hence al the packets should be digitally signed before they are send out and verifies before they are accepted.

IV. PROPOSED SYSTEM

The proposed scheme Advance Enhanced Adaptive Acknowledgment system (SEAACK) is based on previous research EAACK. Compared to existing EAACK advance EAACK advances in following features i.e after analysing EAACK in various scenarios and found that it gave poor performance during.

Scenario 1: Link breakage, occurs due to

1. Continuously changing network topology
2. High mobility of nodes
3. Factors like traffic and delay
4. Nodes move beyond transmission range
5. Insufficient energy levels

Scenario 2: Malicious source node, resulting in

1. Packet drop
2. Drained battery
3. Buffer overflow
4. Message tampering
5. Fake routing
6. Stealing information.

As discussed previously TWOACK and AACK solve weaknesses of receiver collision and limited transmission power but both of them are vulnerable to the false misbehaviour attack. In this proposed work, our goal is to study the Enhanced Adaptive Acknowledgement (EAACK) scheme and analyse the limitation of this scheme. EAACK is an Enhanced intrusion detection system specially designed for MANETs, which solves not only receiver collision and limited transmission power, but also the false misbehaviour problem but it gave poor performance during link breakage and malicious source node.

V. PERFORMANCE EVALUATION

This section concentrates on describing our simulation environment and methodology as well as comparing performances through simulation result

A. *Simulation Methodologies*

To better examine the performance of EAACK under different types of attacks, we intend two scenario settings to simulate different types of misbehaviours or attacks.

Scenario 1: Under link breakage, the existing EAACK scheme fails. Hence, in our proposed scheme, every node maintains a neighbour list. And this list gets updated range, it is identified. Therefore, if that node moves out of communication range, it will not be able to send an acknowledgment to the source. But, still since the neighbour list is being updated periodically, the source will not classify this node as a malicious node. On the other hand, the existing EAACK algorithm does not verify the network condition and thereby identifies the node as a malicious node.

Scenario II: In existing EAACK algorithm, every decision about the intruders is made by the source. Hence, if source is itself an attacker, EAACK has no provision to identify it. Hence in our proposed scheme, the behaviour of every node is recorded and stored as a table. Every node in the network maintains this table about the past history of every other node in the network. Therefore, if the source node is malicious and tries to send data to the other nodes in the network, the nodes will first check the table to find if the node is a malicious node. If that node has already been marked malicious, the data from that node is dropped.

B. *Simulation Configuration*

Our simulation is conceded out within the Network Simulator 2.28 in Windows 7 operating system with NS2 as the interface tool. There are 200 nodes defined in a simulation area of size 1000x1000m. The mobility of nodes is limited to 250ms. The traffic model chosen is Constant bit rate(CBR). The packets are routed using Ad hoc On-demand distance vector routing protocol and the acknowledgments are authenticated using digital signatures

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics.

1) Routing Overhead

Ro defines the amount of routing related

information. Because of high mobility of the nodes in MANETS, always there is a greater chance of frequent link breakages between nodes. These frequent link failures will cause a number of rebroadcasts between nodes which upon build unnecessary routing overhead. thus proposed protocol alleviates the network collision by reducing the routing overhead, so as to Quality of Service (QoS) routing is MANETS is maintained.

2) Throughput

In data transmission network throughput is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps). Throughput increases when connectivity is better .It is observed that performance of TWOACK drastically reduces as compared to SACK and MRA is slightly better than SACK.

C. Performance Evaluation

The graph results obtained after the execution of existing EAACK algorithm for various performance metrics are as follows. Fig. shows how the performance of EAACK degrades in scenarios of link breakage, source maliciousness and partial packet dropping

1) Routing Overhead

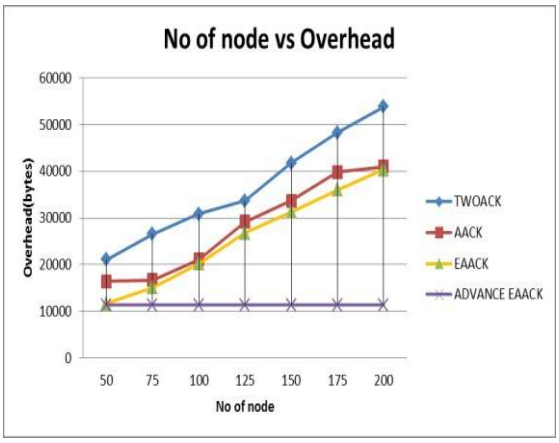

Fig 2 Routing Overhead

From the fig 3, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are having more routing overhead due to packet drop.Our proposed scheme is having least routing overhead in the scenario of link breakage and source maliciousness. Above figure state tha TWOACK is having highest routing overhead this due to time required to send the packets between two node is less while AACK and EAACK scheme is comparatively higher than TWOACK .Above shown graph are in the scenario of link breakage and source maliciousness

2) Throughput

In the second scenario, we set source node as malicious node whenever it is possible. This scenario setting is designed to test the IDS's performance under the source maliciousness. From the fig we can state TWOACK , AACK and EAACK has lowest throughput in terms of link breakage but throughput is maximum seen in our proposed EAACK this is due to constantly updated neighbour list due which less packet drop take place hence less delay and more throughput. With respect to above two result advance EAACK is more desirable scheme in MANETs during link breakage and source maliciousness.

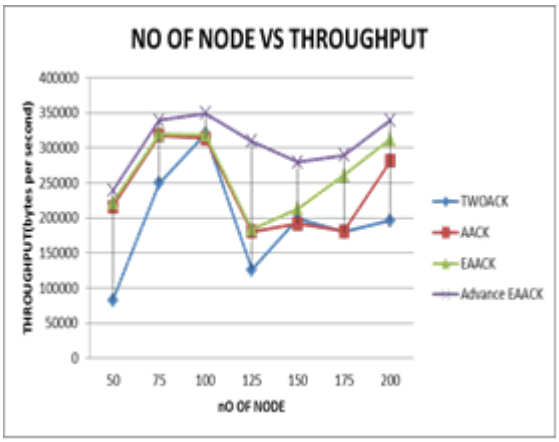

Fig 4 Throughput

V. *CONCLUSION*

Packet dropping is always being the major threat to the security in MANETs. In this paper the main concentration has been laid on comparative study of EAACK approach and its limitation with EAACK protocol using advance EAACK.. The algorithm is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report and to authenticate whether the destination node has received the reported missing packet through a different route and to achieve this we have to focus on the comparative study of ACK, SACK & MRA scheme but in scenario of link breakage and source maliciousness performance of existing EAACK degrades so the proposed protocol advance EAACK is compared against popular mechanism such as TWOACK,AACK and EAACK in different scenario through simulation. Simulation parameters that are considered in this paper is packet delivery ratio and delay. The results demonstrated positive performances against TWOACK, AACK and

EAACK in the cases of link breakage and source maliciousness.

REFERENCES

[1] R. Akbani, T. Korkmaz, and G. V. S. Raju, ―Mobile Ad hoc Network Security,‖ in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[2] R. H. Akbani, S. Patel, and D. C. Jinwala, ―DoS attacks in mobile ad hoc networks: A survey,‖ *in Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[3] T. Anantvalee and J. Wu, ―A Survey on Intrusion Detection in Mobile Ad Hoc Networks,‖ *in Wireless/Mobile Security*. New York: Springer- Verlag, 2008.

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

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

[6] Y. Hu, D. Johnson, and A. Perrig, ―SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, *in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl*., 2002, pp. 3– 13.

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

[8] D. Johnson and D. Maltz, ―Dynamic Source Routing in ad hoc wireless networks,‖ *in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5*, pp. 153– 181.

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, ―Video transmission enhancement in presence ofmisbehaving nodes inMANETs*,‖ Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] N. Kang, E. Shakshuki, and T. Sheltami, ―Detecting misbehaving nodes in MANETs, *in Proc. 12th Int. Conf. iiWAS, Paris, France*, Nov. 8–10, 2010, pp. 216–222.

[11] M. Zapata and N. Asokan, ―Securing *ad hoc* routing protocols, in

Proc. ACM Workshop Wireless Secure., 2002, pp. 1–10

[12] N. Nasser and Y. Chen, ―Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network*,‖ in Proc. IEEE Int.*

Conf. Commun., Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[13] T. Anantvalee and J. Wu, ―A Survey on Intrusion Detection in Mobile Ad Hoc Networks,‖ in *Wireless/Mobile Security*. *New York: Springer-Verlag, 2008.*

[14] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami ―EAACK—A Secure Intrusion-Detection System for MANETS)

[15] N. Kang, E. Shakshuki, and T. Sheltami, ―Detecting forged acknowledgements in MANETs, in Proc. IEEE 25th Int. Conf. AINA,

Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[16] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, ―An acknowledgment-based approach for the detection of routing misbehaviour in

MANETs, IEEE Trans. Mobile Comput., vol. 6, no. 5 pp. 536–550, May 2007.

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