ISSN No. 0976-5697

Volume 5, No. 1, Jan-Feb 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Study on improved version of Enhanced Adaptive Acknowledgement (EAACK) Called EAACK2 in MANETs

Harsha singh*[1], Aditi verma[2], Yesha pruthi[3]
[1,2,3] Computer science and engg,
PDM college of Engg for women, MDUPDM college of engg for women, MDU
Bahadurgarh, Haryana Bahadurgarh, Haryana
er.harshasingh@gmail.com*[1], aditirules123@gmail.com[2], yeshupruthi@gmail.com[3]

Abstract: Mobile ad hoc network (MANET) is a collection of autonomous mobile nodes with infrastructure less network .In MANET, the mobile nodes are equipped with both wireless transmitter and receiver that communicate via bi-directional wireless links. Moreover, the mobile nodes are self configuring and self organizing in nature, these unique characteristics made MANET ideal to be deployed in a remote or mission critical area like military use or remote exploration. However, the open medium, wide distribution of nodes and changing topology and lack of centralizing monitoring in MANET leave it vulnerable to various means of attacks. It is difficult to develop suitable intrusion detection scheme to protect MANET from malicious attackers. In this paper, we introduce an improved version of EAACK called EAACK2 that helps in detecting forged acknowledgement and performs well in the presence of false misbehavior and partial dropping.

Keywords: TWOACK, AACK, EAACK, EAACK2

I. INTRODUCTION

Over the past few years, with the trend of mobile computing, Mobile Ad hoc NETwork (MANET) has become one of the most important wireless communication mechanisms among all. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. Unlike traditional network architecture, MANET does not necessitate a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate with each other when they are both within the same communication range.

A MANET is termed to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In other words a MANETs are self-configuring networks which are perceived as the upcoming technology in scattered networks and ad hoc networking. CurrentlyAd hoc netowrks are enjoying extraordinary research interest,and are expected to provide opportunities for ultilization of network applications in new scenario in which todays internet-based communication paradigms are no longer applicable. As compared to all the wireless networks,MANETs are of unique importance.MANET is a collection of wireless mobile nodes which are each equipped with both a receiver and a transmitter. The individual nodes cooperate with other by forwarding packets when the packets' destination node is beyond the source node's wireless transmission range.

The network topology frequently changes due to the mobility of mobile nodes as they move into or move out of the network. In a MANET, nodes within wireless transmission ranges can communicate easily. However, nodes outside each other's range have to rely on some other nodes to relay messages. Thus, a multi-hop framework occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Each node functions as a router and a host .The success of communication highly depend on nodes cooperation.

The change of communication medium from physical cable to over the air has brought a lot of challenges to the computer communication security research. Due to the distint characteristics like open medium, mobile topology and lack of centralized monitoring, MANETs are especially highly vulnerable to attackers. Most of the proposed routing protocols for MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious. In other words no node maximizes its benefit at the expense of other [3].This assumption inevitably leaves malicious attackers with the opportunity to compromise the entire network by inserting malicious or non-cooperative nodes to MANETs.

A MANET is more vulnerable to attacks as compared to a wired network due to the following factors:

a) Nodes are battery limited due to which complex security solutions cannot be used.
b) Transmission of routing and data packets is done in wireless medium, which is shared and generally unreliable and makes eavesdropping more likely. Even if the channel is reliable, due to the broadcast nature of MANETs the communication may still be unreliable .
c) There is no central management point, which makes it difficult to ensure that all nodes participating in the network .
d) Mobility of nodes plays a very important role in the network, which makes routing even more challenging as the topology keeps changing regularly.

There are two types of attack in MANET:-

a. passive attack:

Packets containing secret information might be tampered, which violates confidentiality.

Examples include monitoring, eavesdropping and traffic analysis.

b. active attack:

Active attack, including injecting packets to invalid destinations into the network, deleting packets, and impersonating other nodes violate availability, modifying the contents of packets, integrity, non-repudiation[9] and authentication

Examples include spoofing, modification, replaying, jamming and Denial of Service (DoS).

An individual mobile node may attempt to take benefit from other nodes, but refuses to share its own resources and maximize their benefit at the expense of all other. Such nodes are called selfish or misbehaving nodes[3].

Intrusion Detection system in MANETS

As discussed earlier, due to the limitations of most MANET routing protocols, MANETs node assumethat other nodes always cooperate with each other to relay data. This belief leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. Toaddress this problem, researchers have devoted their time and effort to develop various Intrusion Detection System (IDS) are designed specially to enhance the security level of MANETs.Mostof the effective mechanisms are derived from Watchdog scheme [5]. The watchdog scheme identifies the misbehaving node by overhearing on the wireless medium is based on passive overhearing.

(a). Watchdog:-

The Watchdog/Path rater is a solution to the problem of malicious nodes in MANET.Watchdog that aims to improve throughput of network with the presence of malicious nodes.

The watchdog scheme is consisted of two parts:-

Watchdog is responsible to detect the misbehaving nodesor selfish nodes. Path rater respond to the intrusion by isolating the selfish node from the network operation[2].

Watchdog scheme serves as an intrusion detection system for MANETs and responsible for detecting malicious nodes misbehaviors in the network. Watchdog identifies malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears its next node fails to forward the packet within a certain period of time, it increasesits failure counter. Whenever failure counter exceeds a predefined threshold, the Watchdog node announce it as misbehaving and the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Watchdog scheme fails to detect misbehaviors with the presence of:

i. Ambiguous collisions,
ii. Receiver collisions,
iii. Limited transmission power,
iv. False misbehavior report,
v. Collusion,
vi. Partial dropping.

For ambiguous collisions, Node A may fail to overhear the transmission of node B due to collisions from Packet 2, as demonstrated in Figure 4. Please note that for rest of this paper, all dotted arrow lines in the figure indicate the transmission is that actually involved in our discussion.

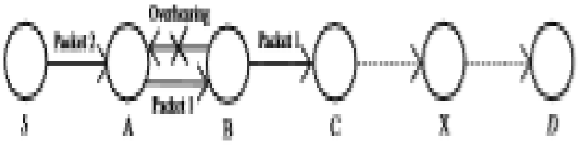


Figure 4. Ambigous Collisions.

For receiver collisions, node A overhears that's node B has successfully forwarded packet 1 to node C, but failed to detect that node C did not receive packet 1 due to collision with packet 2,as demonstrated in figure 5.

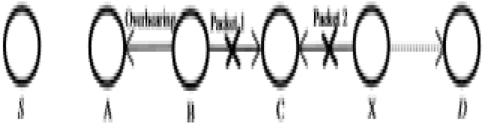


Figure 5. Receiver Collisions.

For limited transmission power ,in order to preserve its own battery, node B limits its transmission power so that node A can overhear the transmission, but it is not strong enough for node C to receive Packet 1, as shown in Figure 6.

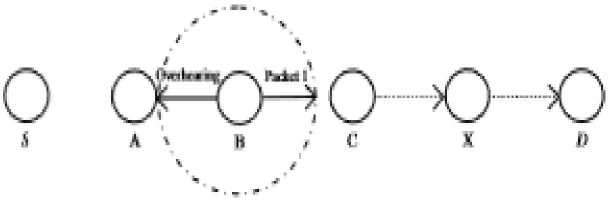


Figure 6. Limited Tranmission Power

In false misbehavior report, node B successfully forwarded Packet 1 to node C, and node A overhears that, but node A still reports node B as misbehaving. Due to the open medium of MANETs, attackers can easily capture one node and achieve this misbehaving report attack. Figure 7 described this process.

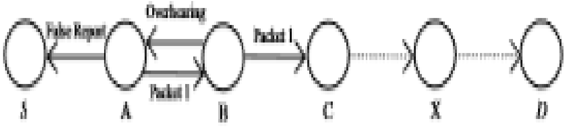


Figure 7. False Misbehavior

A. Two ack:

The purpose of TWO ACK is to resolve the receiver collision and limited transmission power problems of watchdog. TWO ACK detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the path from the source to the destination. On retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWO ACK[7] scheme can be added into source routingprotocols like DSR(Dynamic source routing).The working process of TWOACK indicated, node A first forwards packet 1 to node B, and then node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is require to generate a TWOACK packet which contains reverse route from node A to node Cand sends it back to node A. The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Else if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.Although TWO ACK solves the problem of detecting malicious nodes in the presence of collision and limited transmission power but still vulnerable to false misbehavior nodes.

B. Aack:

AACK[7] is another very important IDS specially designed for MANETs.It is an acknowledgement based network scheme which is considered as combination of TWOACK and end to end acknowledgement scheme.AACK managed to reduce network overhead as compared to TWOACK but they both fail to detect malicious nodes with presence of false misbehavior report and forged acknowledgement packets.

C. Eaack:

The purpose of EAACK[8] is to tackle three out of six weaknesses of watchdog scheme, namely false misbehavior,limited transmissionpower and receiver collision .EAACK is introduced with digital signature to prevent the attacker from forging acknowledgement packets. EAACK is divided into three parts:-

a. 1.Acknowledge(ACK)
b. 2. Secure-Acknowledge(S-ACK)
c. 3.Misbehaviour ReportAuthentication(MRA)

D. Ack:

In ACK mode, node S first sends out an ACK data packet ad P to the destination node X. If all the intermediate nodes along the route between node S and node X are cooperative and node X successfully receives ad P, node X is required to send back an ACK acknowledgement packet ak P along the same route but in a reverse order. Within a given time period, if node S receives ak P, then the packet transmission from node S to nodeX is successful. Else, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.ACK is basically an end-to-end acknowledgement scheme.it is very important in EAACK ,aiming to reduce network overhead .

E. S-ack:

S-ACK scheme is an improved version of TWOACK scheme proposed by Liu et al. The principle is to let each three consecutive nodes work in a group to detect misbehaving nodes. For each three consecutive nodes in the route, the third node is necesiate to send an S-ACK acknowledgement packet to the first node. The purpose of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

As demonstrated in Fig. 8, in S-ACK mode, the three consecutive nodes (i.e. F1, F2 and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends S-ACK data packet to node F2. Then node F2 convey this packet to node F3. When node F3 receives , as it is the third node in this three-node group, node F3 is needed to send back an S-ACK acknowledgement pack- et to node F2. Node F2 forwards back to node F1. If node F1 does not receive this acknowledgement packet within a predefined time period, both nodes F2 and F3 are re- ported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. 1 s adP 1 s adP 1 s akP 1 s akP .

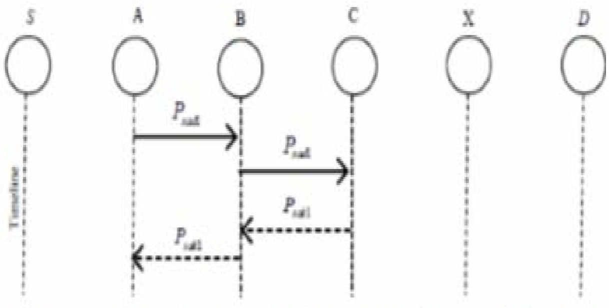


Fig. 8. S-ACK Scheme: node C is required to send back an acknowledgement packet to node A.

Detect misbehaving nodes in the network. Node F1 first sends S-ACK data packet s ad1 P to node F2. Then node F2 forwards this packet to node F3. When node F3 receives s ad1 P , as it is the third node in this three-node group, node F3 is needed to send back an S- ACK acknowledgement packets ak1 P to node F2. Node F2 forwards s ak1 P back to node F1. If node F1 does not receive the acknowledgement packet within predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S.Nevertheless, unlike TWOACK scheme, where the source node imme- diately trusts the misbehavior report, EAACK necessiate the source node to switch to MRA mode and confirm this misbehavior report. This is a important step to detect false misbehavior report in our proposed scheme.

F. Mra:

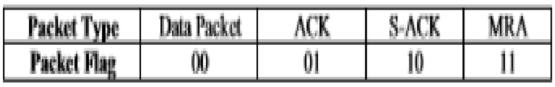
The Misbehavior Report Authentication (MRA) scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report.False misbehavior report can be generated by malicious attackers to falsely report that innocent nodes as malicious. This attack can be deadly to the entire network when the attackers break down sufficient nodes and thus cause a network division. The main MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

The previous approach EAACK is designed to tackle three of the six weakness of Watchdog Scheme,i.e false misbehaviour , limited transmission power, and recevier collosion.In this section, we discuss proposed Enhanced Adaptive ACKnowledgement version 2(EAACK2) scheme.This scheme is the advance version of EAACK scheme in the following way:

a. 1.Acknowledgement authentication:Prevents attackers from forging fake acknowledgement packet.
b. 2.Packet integrity: Prevents attackers from contaminating packets in MANETs.
c. 3.It tackles all the six weakness of Watchdog scheme namely ambiguous collisions,recevier collisions,limited transmission,false mesbehaviour,collusion,partial droping.

Please note that in our proposed scheme, we assume that links between each node in the network is bi-directional. All malicious nodes are intermediate nodes; they are neither the destination node nor the source node in three-hop acknowledgement process. Misbehaving nodes cooperate in the routing stage while dropping all data packets. To conceive the source node and protect itself, after dropping data packets, malicious nodes always generate a forged acknowledgement packet and send it back to the source node. The purpose of such settings is to evaluate the performance of our proposed scheme in the worst scenario.EAACK2 scheme is mainly divided into three parts, namely ACK,S-ACK and MRA.EAACK2[1] scheme starts with ACK mode.The source node first searches its local memory to see if there are any existing routes leading to the destination node. If yes, data packets are sent along one of these routes. If not, it uses DSR to find a new route. These data packets contain a two bit header that indicates the packet type. In our case, general data packet has a header of “00”, ACK packet is “01”, S-ACKas“10” and MRApacket as“11”.This is listed in Table 1

Table 1. Packet Type Flags



Packet Type	Data Packet	ACK	S-ACK	MRA
Packet Flag	00	01	10	11

When source node sent data packet to the destination node , it also register the packet ID and sent time in its local memory.On receiving a data packet at destination node,it is required to send back an acknowledgement packet i.e ACK packet which contains the packet ID.If source node receives ACK packet within the timespan ,then transmission is completed successfully.However,after a certain time out ,if the source node does not recevies the desired packet from the destination node,it switches to S-ACK mode by sending an S-ACK packet to the destination through the same route.

The S-ACK mode is based on the TWOACK [7] scheme. For every three consecutive nodes along the transmission route, the third node is necessitate to send back an S-ACK packet back to the first node to confirm receiving the packet. Unlike what we did in EAACK, where all positive acknowledgements are accepted without doubt, in EAACK2, the third node is required to sign this S-ACK packet with its own digital signature. The purpose of doing this is to prevent the second node from forging the S-ACK packet without forward the packet to the third node. This is really dangerous as the malicious node can create a black-hole in the network without being detected. When the first node receives this S-ACK packet, it certifies the third node’s signature with the predistributed public key. On the other hand, if no S-ACK packet is received within a pre- defined time period; the first node will report both second node and the third node as malicious.

When the source node receives the malicious report, inspite of trusting the report immediately and marks the nodes as malicious, EAACK2 requires the source node to switch to MRA mode to confirm. The source node switches to MRA mode by sending out an MRA packet to the destination node via a alternate route. If such route does not exist in the cache, the source node initiates a new DSR route request to find a new route. The MRA packet contains the data packet ID. When destination node receives the MRA packet, it searches through its local memory to find out whether the requested packet ID exists. If yes, then the data packet has been received and whoever sent the report is the real misbehaving node. Otherwise, the misbehavior report is confirmed. For extreme conditions when there are no alternative routes from source node to the destination node, EAACK2, by default, accepts the misbehaving report.

We describe the following steps in which EAACK2 scheme works:-

Step 1: the source node sends ACK packet to the destination node

Step 1.a:If the source node receives ACK paback cket from the destination node within the required timespan.the transmission is successful.

Step1.b: After certain time out ,if the source node does not recevies ACK packet from destination node then switch to S-ACK mode

Step2: In S-ACK mode, third node send S-ACK packet to the first node along with its own digital signature.When the first node receives S-ACK packet,it verifes the third node signature with predistributed key.

Step2.a:If verification is correct then transmission is successful.

Step 2.b:Otherwise , a misbehaviour report is generated which says second and third node are malicious node.

Step3: Instead of trusting the report immediately switch to MRA mode.The souce node send out MRA packet to the destination node via different path using DSR routing technique.

Step3.1: After receiving MRA packet ,the destination node searches in its local memory to find out whether requested packet ID exists or not.

Step3.1.a: If data packet exists in its local memory then whoever sent the report is real misbehaving node.

Step3.1.b: Otherwise , trust the misbehaviour report.

Step 3.2: If no other alternative route exist then by default accepts misbehaving report.

II. CONCLUSION

In this survey paper, a comparative study of Intrusion-Detection Systems (IDS) for discovering malicious nodes . Due to some special characteristics of MANETs,prevention mechanisms alone are not adequate to manage the secure networks. In this, detection should befocused as another part before an attacker can damage the structure of the system. we study about secure IDS named EAACK2 protocol specially designed for MANETs . Security is major part in MANETS, hybrid cryptography architecture will confront the issue in an efficient manner.By This way we can better preserve battery and memory space of mobile nodes.Moreover,EAACK2 performes better in the presence of forged acknowledgement packets and assures packet integrity when potential attack occurs.

III. ACKNOWLEDGEMENT

The author would like to thankU. SharmilaBegam, Dr. G. Murugaboopathi.A recent secure instrusiondetection system on manet.International Conference on Information Systems and Computing (ICISC-2013) without their paper its difficult to write this paper.

IV. REFERENCES

[1]. N. Kang, E. M. Shakshuki and T. R. Sheltami. Detecting Forged Acknowledgement in MANETs .In IEEE 2011

[2]. R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Net- work Security", Lecture Notes in Electrical Engineering, vol. 127, pp. 659-666, Springer, 2012

[3]. L. Buttyan and J.P. Hubaux. Security and cooperation in wireless networks. Cambridge University Press, August, 2007

[4]. K. Liu, J. Deng, P.K. Varshney and K. Balakrishnan. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. IEEE Transactions on Mobile Computing, May, 2007, 536-550, DOI=http://dx.doi.org/10.1109/TMC.2007.103606 - 11, 2000, MobiCom '00. ACM, New York, NY, 255-265.

[5]. S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual inte Mobile Computing and Networking, Boston, Massachusetts, United States, August.

[6]. B. Wu, J. Chen, J. Wu and M. Cardei. A survey of attacks and countermeasures in mobile ad hoc networks.Wireless Network Security, Xiao, Y., Shen, X. and Du, -Z, D. Net. 2006

[7]. T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mohmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282. 2009.

[8]. N. Kang, E. M. Shakshuki and T. R. Sheltami. Detecting Misbehaving Nodes in MANETs, the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), November, Paris, France.

[9]. U. Sharmila Begam, Dr. G. Murugaboopathi. A recent secure intrusion detection system on manet. International Conference on Information Systems and Computing (ICISC-2013), INDIA.