ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 06|| June – 2016 ||
International Journal of Computational Engineering Research (IJCER)

Performance Enhancement of Intrusion Detection System Using Advance Adaptive EAACK for MANETs

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 are very sensitive to security threats due to their nature of deployment such as open wireless system. MANETs have self-configuring ability of nodes and infrastructure less nature hence they are preferred in significant applications. This itself emphasizes the importance of security and the need for an efficient intrusion detection system in MANETs. Many IDS have been proposed for detecting malicious nodes. On such different IDS, Enhanced Adaptive Acknowledgment (EAACK) has overcome the drawbacks of Watchdog, ACK and TWOACK. In our proposed work we have identified the inadequate nature of EAACK in scenarios of link breakage, source maliciousness. High mobility of MANET nodes contributes to frequent link breakages in the network which leads to path failures and route discovery processes difficult. Route discovery is initialized through broadcast mechanism usually. In this paper a new intrusion detection system is proposed named Advance EAACK particularly designed for MANETs. Compared to modern approaches, advance EAACK demonstrates higher malicious behavior detection rates in certain conditions while does not affect the network performance greatly. Due to this mechanism data transformation between mobile nodes are done with improved or high security .Parameters going to measure network performance are packet delivery ratio and delay.

Keywords: *Adaptive acknowledgment (AACK), Dynamic source routing (DSR) , Digital Signature Algorithm (DSA),EAACK (Enhanced Adaptive Acknowledgment) ,Misbehavior Report Analysis (MRA),MANETS (Mobile Ad-hoc Networks) , IDS (Intrusion detection system)*

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-organizing and self-configuring multi-hop wireless network, where the nodes are free to move randomly. Ad hoc wireless network are self-creating and self-organizing. One advantage of wireless networks is the ability to transmit data among users in a local area while remaining mobile. The communication between the nodes is limited to their range of transmitter. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem they allow intermediate node to transmit data between two other nodes. To achieve this by MANETs are divided into two types into two types of networks, namely, single-hop and multi-hop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has no fix structure; thus, all nodes are free to move randomly.

MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure and are many used in critical applications like military conflict or emergency recovery. Thus Minimal configuration and quick arrangement make MANET ready to be used in emergency circumstances where an infrastructure is not easy to arrange in scenarios like natural or human induced disasters, military conflicts, and medical emergency situations. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET[1][2] is becoming popular among critical mission applications, network security is of most importance. Because of open medium and remote distribution of nodes in MANET they are vulnerable to various types of attacks. For example, due to the nodes lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering most routing protocols in MANETs behaves cooperatively with other nodes

and not malicious, attackers can easily compromise MANETs by inserting malicious or no cooperative nodes into the network. Moreover due to distributed nature of market centralized monitoring system is not feasible. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANET
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. Lastly, conclusions drawn from the paper and future work are given in Section V.

II. RELATED WORK

A. Intrusion Detection System in MANETS.

As discussed before nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve one or two compromised nodes in the network. To address this problem, Intrusion Detection System (IDS) [3] should be added to enhance the security level of MANETs. Intrusion detection is the process of identifying the actions which are going to compromise the integrity, confidentiality, and availability of a resource i.e. nothing but the security verification. Intrusion detection systems should be added to enhance and improve the level of the security in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog, TWOACK and AACK.

B. *WATCHDOG*

Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) Ambiguous collisions 2) Receiver collisions 3) Limited transmission power 4) False misbehavior report 5) Partial dropping.

C. TWOACK

TWOACK is neither an enhancement nor a Watchdog based scheme. Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK [7] detects misbehaving links by acknowledging each data packets transmitted over each three consecutive nodes along the path from the source to the destination upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK works on routing protocols such as Dynamic Source Routing (DSR) [8]. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. But, the acknowledgement process is time consuming and add network overhead in the scheme and due to limited battery power nature of MANETs easily degrades the life spam of entire network.

D. *AACK*

Similar to TWOACK, AACK is an acknowledgement based network layer scheme which can be considered as a combination of a scheme call ACK (identical to TWOACK) and an end-to-end acknowledgement scheme called ACK [9]. Compared to TWOACK, AACK reduces network overhead and maintain network throughput. The concept of hybrid scheme is adopted in AACK which greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

III. EXISTING SYSTEM

In this section, enhanced Adaptive Acknowledgement (EAACK) scheme is detailed. The approach described in this research paper is based on our previous work [10], where the backbone of Advance EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

A. ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It is a hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected.

B. S-ACK

The S-ACK scheme is improved version of the TWOACK scheme. It works on the principle that every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA

The MRA scheme is designed to solve weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This scheme authenticate whether the destination node has received the reported missing packet through another route. For that, we first search for an alternative route to destination. Then sent a MRA packet from S to D through that alternative path. After receiving in the destination, it searches its local knowledgebase and compares if the reported packet was received. If it was already received, then it concludes that this report is false report and marks the node whoever generates this report as malicious. Then avoid the malicious node in future transmission. In MANET we can find multiple paths between pair of nodes. By choosing an alternative route source can send the misbehavior reporter node. When the node D receives an MRA packet, it looks in to its local knowledge base and check if the reported packet was received. If it is received, then conclude that this report is a false misbehavior report and reporter, whoever generated this report is marked as malicious node. Otherwise, report is trusted and accepted. By MRA scheme, EAACK can detect malicious nodes even in the presents of false misbehavior report.

D. Digital Signature

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, all packets are authorized and authenticate. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this,we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

IV. PROPOSED WORK

In this section we propose Advance Enhanced Adaptive Acknowledgment system (SEAACK). This scheme is based on our previous research EAACK. Compared to EAACK advance EAACK advances in following features i.e. after analyzing EAACK in various scenarios and found that it gave poor performance during.

Scenario 1: Link breakage, occurs due to continuously changing network topology, high mobility of nodes, factors like traffic and delay, nodes move beyond transmission range, insufficient energy levels

Scenario 2: Malicious source node, resulting in packet drop drained battery, butter overflow, message tampering, fake routing and stealing information.

As discussed in previous sections, TWOACK and AACK solve weaknesses, namely receiver collision and limited transmission power. However, both of them are vulnerable to the false misbehavior attack. In this research work, our goal is to study the Enhanced Adaptive Acknowledgement (EAACK) scheme and analyze the limitation of this scheme. As per previous work the 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 misbehavior problem but it gave poor performance during link breakage and malicious source node.

V. PERFORMANCE EVALUATION

In this section, we concentrate on describing our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, and EAACK schemes

A. Simulation Methodologies

To better investigate the performance of EAACK under different types of attacks, we propose two scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: Under link breakage, the existing EAACK scheme fails. Hence, in our proposed scheme, every node maintains a neighbor list. And this list gets updated periodically, so that when nodes move out of communication 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 neighbor 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 behavior 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 carried out within the Network Simulator 2.28 in Windows Xp operating system with NS2 as the interface tool. There are 200 nodes defined in a simulation area of size 1000x1000. The mobility of nodes is limited to 250ms. The traffic model chosen is Constant bit rate. The packets are routed using Ad hoc On-demand distance vector routing protocol and the acknowledgments are authenticated using RSA algorithm

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

1) Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node
2) Delay: Network delay is an important design and performance characteristic. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another.

C. Performance Evaluation

Results

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) Packet Delivery Ratio

From the fig 2, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to provide good packet delivery ratio but not as good as compared to our proposed scheme .Above figure TWOACK is having least PDR 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.

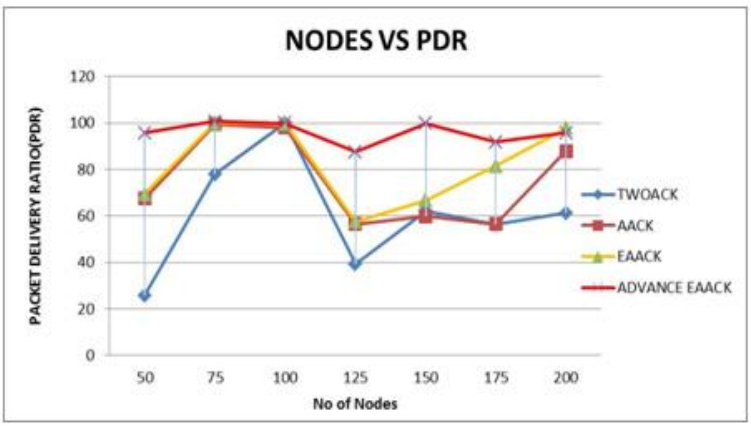

Figure 1 Packet Delivery Ratio

2) Delay

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.

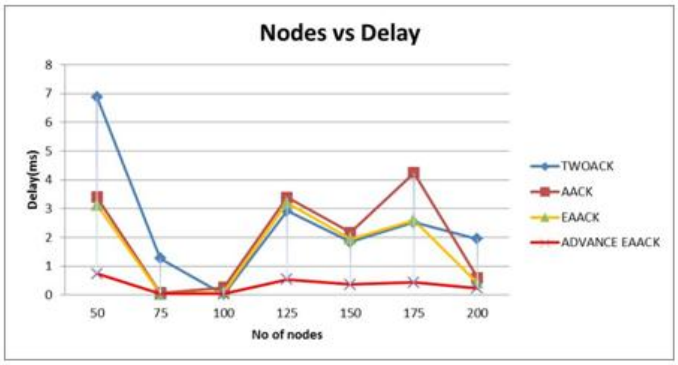

Figure 2 Delay in advance EAACK

From the fig we can state TWOACK, AACK and EAACK has more delay in terms of link breakage but delay is least seen in our proposed EAACK this is due to constantly updated neighbor list due which less packet drop take place hence less delay in packet to reach the destination With respect to above two result advance EAACK is more desirable scheme in MANETs during link breakage and source maliciousness.

VI. CONCLUSION

In this paper the main focus has been laid on comparative study of EAACK approach and its limitation with EAACK protocol using advance EAACK. Here we have study the behavior of EAACK technique. 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.

REFRENCES

[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.

[18]. L. Zhou and Z. Haas, ―Securing ad-hoc networks,‖ IEEE Netw., vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999. Botan, A Friendly C ++ Crypto Library. [Online]. Available: http://botan.randombit.net/.