ENHANCED ADAPTIVE ACKNOWLEDGEMENT FOR DETECTING INTRUSION USING A HYBRID ALGORITHMS IN MANETS

[1]S.Saravanan, [2]S.Vanitha

[1]PG Scholar, Department of ECE, SNS College of Technology, Coimbatore

[2]Assistant Professor, Department of ECE, SNS College of Technology, Coimbatore

[1]Saravanaa.25@gmail.com, [2]vanitharajanneel@gmail.com

Abstract: Mobile Ad hoc Network (MANET) is one of the most important and unique applications. The self-configuring ability of nodes in mannet made it popular among critical mission applications like military use or emergency recovery. A new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs was implementing in this paper. Using this approach, EAACK demonstrates higher malicious- behavior- detection rates in certain circumstances while does not greatly affect the network performances. Since it is not feasible in MENET we introduce a new concept called Blowfish algorithm in this paper. Blowfish is a new method to enhance the security. And it will provide better results against any type of intrusion.

Index Terms: EAACK, Blowfish, malicious behavior, intrusion, attack.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Industrial remote access and control via wireless networks are becoming more and more popular these days.

One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. 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 by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET 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 a decentralized network infrastructure. MANET does not require a fixed infrastructure; 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, which is often infeasible in critical mission applications like military conflict or emergency recovery.

Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

1.1 Advantages

Have in discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

- Low cost of deployment: As the name suggests, adhoc networks can be deployed on the fly, thus requiringno expensive infrastructure such as copper wires, data cables, etc.
- Fast deployment: When compared to WLANs, adhoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.
- Dynamic Configuration: Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms ,etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

Intrusion Detection system in MANETS due to the limitations of most MANET routing protocols, 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 significant impact on the network with just one or two compromised nodes. To solve the problem, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes at the first time. IDSs usually act as the second layer in MANETs, and it is a great complement to existing proactive approaches and presented a very thorough survey on contemporary IDSs in MANETs. In this section, we mainly describe three existing approaches, namely, Watchdog,

1.2 TWOACK and AACK.

Watchdog that aims to improve the throughput of network with the presence of malicious nodes. Watchdog scheme is consisted of two parts, namely Watchdog and Path rater. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path rater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. We choose this metric because it gives a comparison of the overall reliability of different paths and allows path rater to emulate the shortest length path algorithm when no reliability information has been collected, as explained below. If there are multiple paths to the same destination, we choose the path with the highest metric.

Watchdog scheme fails to detect malicious misbehaviors with the presence of the following

- Ambiguous collisions
- Receiver collisions
- Limited transmission power
- False misbehavior report
- Collusion
- Partial dropping.

1.3 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 detects misbehaving links by acknowledging every 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 acknowledgement packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR).

The working process of TWOACK is demonstrated in Fig. 1, 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 obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node

The retrieval of this TWOACK packet at node A indicates the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in predefined time period, both nodes B and C are reported malicious. TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgement process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire net work

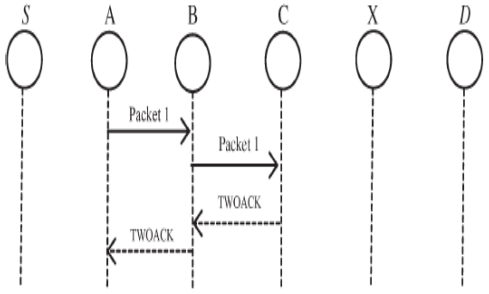

Figure 1: Twoack

1.3 Aack

It is based on TWOACK Acknowledgement (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. Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. Source node S will switch to TACK scheme by sending out a TACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network over-head, 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 acknowledgement packets. In fact, many of the existing IDSs in MANETs adopt acknowledgement based scheme, including TWOACK and AACK. The function of such detection schemes all largely depend on the acknowledgement packets. Hence, it is crucial to guarantee the acknowledgement packets are valid authentic. To address this concern, to adopt digital signature in proposed scheme EAACK.

1.4 SCHEME DESCRIPTION

EAACK was proposed and evaluated through implementation. In this work, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: Acknowledge (ACK), Secure- Acknowledge (S-ACK) and misbehavior Report Authentication (MRA). In order to distinguish different packet types in different schemes, we included a two-bit packet header in EAACK. According to the Internet draft of DSR , there are six bits reserved in DSR header. In EAACK, we use two of the six bits to flag different type of packets.

1.5 Ack

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 misbehavior is detected

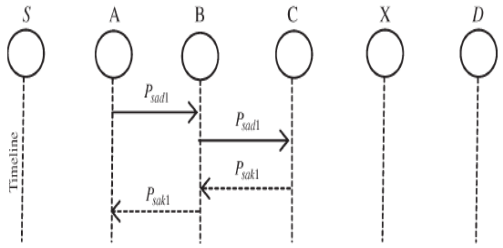

Figure 2: ACK scheme

In Fig. 2, in ACK mode, node S first sends out an ACK data packet Pad1 to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node successfully receives Pad1, node D is required to send back an ACK acknowledgement packet Pak1along the same route but in a reverse order. Within a predefined time period, if node S receives Pak1, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

1.6 S-Ack

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

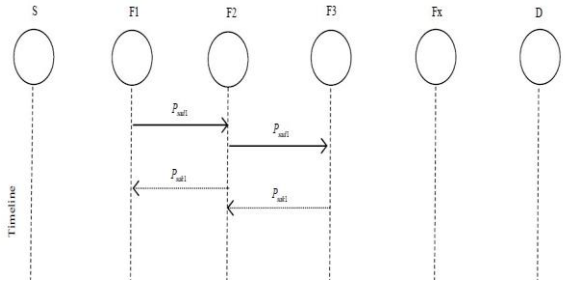

Figure 3: S-ACK scheme

Detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet s ad1 P to node F2. Then node F2 forwards this packet to node F3. When node F3 receives Ps ad1 , as it is the third

node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packets Pak1 to node F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this 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 immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA mode and confirm this misbehavior report. This is a vital step to detect false misbehavior report.

1.7 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 lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. When the destination node receives an MRA packet, it searches its local knowledge base and compare if the reported packet was received. If it is already received, then it is safe to conclude this is a false misbehavior re-port and whoever generated this report is marked as malicious. Otherwise, the misbehavior report is trusted and accepted.

1.8 Digital Signature

EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, SACK and MRA are acknowledgement based detection schemes. They all rely on acknowledgement packets to detect misbehaviors in the network. Thus, it is extremely important to ensure all acknowledgement packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgement packets, all of the three schemes will be vulnerable. With regarding to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgement packets to be digitally signed before they are sent out, and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature scheme in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

2. 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.

2.1 Simulation Methodologies

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

2.2 Scenario 1:

In this scenario, we simulated a basic packet dropping attack. Malicious nodes simply drop all the packets they receive. The purpose of this scenario is to test the performance of IDSs against two weaknesses of Watch-dog; namely, receiver collision and limited transmission power.

2.3 Scenario 2:

This scenario is designed to test IDSs' performances against false misbehavior report. In this case, malicious nodes always drop the packets they receive and send back a false misbehavior report whenever it is possible.

2.4 Scenario 3:

This scenario is used to test IDSs' performances when the attackers are smart enough to forge acknowledgement packets and claiming positive result while in fact it is negative. As Watchdog is not an acknowledgement based scheme, it is not eligible for this scenario setting.

3. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. IDS named EAACK

protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, the research is extended to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. This tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, DSA and RSA schemes are implemented in the simulation. Eventually, the DSA scheme is more suitable to be implemented in MANET.

In Future we investigate the following issues. To analyze the possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature. The hybrid schemes HMAC and BLOWFISH algorithms are going to be used. Also to examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys to test the performance of EAACK in real network.

REFERENCES

[1] EAACK – A Secure Intrusion Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang and Tarek R. Sheltami, Member, IEEE.\

[2] R. Akbani, T. Korkmaz and G.V.S Raju. "Mobile Ad hoc Network Security", Lecture Notes in Electrical Engineering, vol. 127,pp. 659-666,Springer, 2012 – here1

[3] R.H. Akbani, S. Patel, D.C. Jinwala. "DoS Attacks in Mobile AdHoc Networks: A Survey", the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak,Haryana, India. 2012. –here1

[4] T. Anantvalee and J. Wu. A Survey on Intrusion Detection in Mobile Ad hoc Networks. In Wireless/Mobile Security, Springer,2008.

[5] L. Buttyan and J.P. Hubaux. Security and Cooperation in Wireless Networks. Cambridge University Press, Aug. 2007.

[6] N. Kang, E. Shakshuki and T. Sheltami. Detecting Misbehaving Nodes in MANETs. The 12th International Conference on Information Integration and Web based Applications & Services (iiWAS2010), ACM, pp. 216-222, November, 8-10,Paris, France, 2010.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. In the IEEE Transactions on Mobile Computing, vol. 6, pp. 536- 550, 2007.

[8] N. Nasser and Y. Chen. Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad hoc NET work. In the Proceedings of IEEE International Conference on Communication (ICC '07), Glasgow, Scotland, 2007.

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

[10] Y. Xiao, X. Shen, and D. Du (Eds.). A Survey on Intrusion Detection in Mobile Ad-hoc Networks. In Wireless/Mobile Network Security, pp. 170-196, 2006.