A PERFORMANCE IMPROVEMENT FOR MANET USING SECURED ALGORITHM

A.Vijayalakshmi#1, M.E communication systems, K.Ramakrishnan college of engineering, Trichy, India.

#1Vijikartik077@gmail.com

Mr. T. Muruganantham#1 M.E., Assistant professor of ECE, K.Ramakrishnan college of engineering, Trichy, India.

#1tmurgssvm@gmail.com

Abstract— Mobile Ad hoc Network (MANET) is a collection of mobile nodes that communicate with each other. The open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. To protect from attacks they developed Intrusion detection system of Enhanced adaptive acknowledgement it leads to network overhead. The proposed scheme is AUTOSAR algorithm is used to overcome the enhanced adaptive Acknowledgement problem. It improves the performance metrics.

Keywords—AUTOSAR, Fault initializing, Fault rectification

I. INTRODUCTION

Due to the mobility and scalability, wireless networks are always preferred. Due to the improved technology and reduced costs, wireless networks preference over wired networks in the past few decades. Mobile Ad-hoc Network (MANET) is a collection of mobile nodes operational with both a wireless transmitter and a receiver that communicate with each other through bidirectional wireless links either directly or in some way. Industrial remote access and control through wireless networks are fitting. Advantages of wireless networks are ability to allow data communication between different parties and maintain their mobility. Communication is limited to the range of transmitters. 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 multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. Unfortunately, the open medium and remote distribution of MANET make it 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. Furthermore, because of MANETs distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

II. BACKGROUND

A. Intrusion detection system in MANET

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 address this 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 they are a great complement to existing proactive approaches; mainly describe three existing approaches, specifically Watchdog scheme, TWOACK and Adaptive ACKnowledgment (AACK).

1. Watchdog scheme
Watchdog scheme that aims to improve the throughput of network with the presence of malicious nodes. The Watchdog scheme is consisted of two parts namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is conscientious for detecting malicious node misbehaviors in the network. Watchdog detect malicious misbehaviors by listening to its next hop’s transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Every time a node’s failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this crate, the Pathrater cooperate with the routing protocols to avoid the reported nodes in future transmission.

2. **Two Acknowledgement scheme**

TWOACK is neither an enhancement nor a Watchdog-based scheme. aim to resolve the receiver collision and limited transmission power problems of Watchdog. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the Destination. Upon rescue 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 is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is shown 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 indebted to create a TWOACK packet which contains reverse route from node A to node C and sends it back to node A.

The recovery of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. or else, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The same procedure applies to every three uninterrupted nodes along the respite of the route. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems by watchdog.

3. **Adaptive Acknowledgement scheme**

AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

In the ACK scheme is shown in Fig. 2, the source node S sends out Packet 1 without any overhead except of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out a TWOACK packet. The concept of adopting a hybrid scheme in AACK 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.

4. **Digital signature**

Digital signatures have always been an integral part of cryptography in history. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. The development of cryptography technique has a long and fascinating history. Digital signature schemes can be mainly divided into the following two categories.
1) The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA).

2) Another scheme does not require any other information besides the signature itself in the verification process. Examples include RSA. The general flow of data communication with digital signature. First, a fixed-length message digest is computed through a pre agreed hash function $H$ for every message $m$. This process can be described as

$$H(m) = d$$

(3.1)

Second, the sender Alice desires to apply its own private key $P_r_{Alice}$ on the compute message digest $d$. The result is a signature $Sig_{Alice}$, which is attached to message $m$ and Alice’s secret private key

$$S_{Pr_{-Alice}} = Sig_{Alice}$$

(3.2)

To ensure the validity of the digital signature, the sender Alice is obliged to always keep her private key $P_r_{Alice}$ as a secret without revealing to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice’s signature and send them to Bob. As these malicious messages are digitally signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can readily achieve malicious attacks to Bob or even the entire network.

Next, Alice can send a message $m'$ along with the signature $Sig_{Alice}$ to Bob via an unsecured channel. Bob then computes the received message against the pre agreed hash function $H$ to get the message digest $d'$. This process can be generalized as

$$H(m') = d'$$

(3.3)

Bob can verify the signature by applying Alice’s public key $Pr_{Alice}$ on $Sig_{Alice}$, by using

$$S_{Pr_{-Alice}}(Sig_{Alice}) = d.$$  

(3.4)

If $d = d'$, then it is safe to claim that the message $m'$ transmitted through an unsecured channel is indeed sent from Alice and the message itself is intact.

B. Proposed system

1. AUTOSAR Controller
When performing a AUTOSAR run over a window we preload the MISR with the predicted initial value for the start of the window and initialize the pseudo random pattern generator, the pattern counter and stop value for the window.

2. **Fault initializing**

When the AUTOSAR controller is in diagnostic mode it waits, at the end of each AUTOSAR pattern, for the logical interface to perform a data register load/unload shift sequence. Once the sequence has been performed the AUTOSAR controller continues to the next pattern. It is this waiting that provides synchronization between the execution of the AUTOSAR patterns and activity occurring externally that is gathering the information for the diagnostic process. These synchronization points allow diagnostics to be performed from the external interface.

3. **Fault observation**

At AUTOSAR creation time test vectors to run the full AUTOSAR session and observe the value are created. These vectors are used. A failure observe the expected value indicates that the Nodes contains observable faults. Four Step Logic AUTOSAR Diagnostic Process These full AUTOSAR session vectors are compact in nature and perform the operations as shown in the pseudo code below:
4. **Fault classification**

Use the AUTOSAR controller in diagnostic mode to identify the AUTOSAR patterns that cause the information to observe a faulty value. A second set of test vectors, generated at AUTOSAR creation time, run the AUTOSAR in diagnostic mode. These vectors initialize the AUTOSAR controller and then perform the actions described in the pseudo code below:

- Reset AUTOSAR controller
- Initialize AUTOSAR controller
- For each AUTOSAR pattern
  - Wait for 1 AUTOSAR pattern to complete
  - Unload information and reload expected value
  - Verify AUTOSAR signature is expected

These vectors are compact, the bulk of them only contain expected MISR values. If this set of vectors is too large for the test environment it can safely be split into a number of subsets. Just like conventional ATPG vector based ATE application these failing pattern discovery vectors can be prematurely terminated once a sufficient quantity of failing patterns have been discovered.

5. **Fault rectification**

This step requires a third set of vectors, these can be swiftly generated once the failing AUTOSAR pattern set has been identified. This step uses the failing patterns, or a subset of them, and a selection of expected passing patterns. The vectors of this step use the AUTOSAR controller to initialize the scan chains within the core under test and perform the AUTOSAR capture cycle. Then, the vectors unload the scan chain contents and comparing them to the expected scan chain contents for the pattern. This is shown in the pseudo code below:

- Reset AUTOSAR controller
- For each failing AUTOSAR pattern
  - Initialize AUTOSAR controller pattern
  - Wait for AUTOSAR pattern to complete
  - Unload core scan chain contents
  - Verify core scan chain against
  - Expected value

For a large number of failing AUTOSAR patterns this vector set may become sizable. Since diagnostic inference can produce reliable deductions with a small number of failing patterns, it is expected that only a subset of failing AUTOSAR patterns will be unloaded for further analysis. In order to ensure that the AUTOSAR controller is operating correctly the vector set contains a number of significant known passing patterns, within the scan chain integrity test1 and each of the MTPI phases. If these patterns are not unloaded correctly then it is most likely that a defect within the AUTOSAR hardware is preventing correct operation of the AUTOSAR. Access to the DUT scan chains is through either the concatenated single scan chain or the DUT scan chains presented at the level.
of the AUTOSAR DUT. When the AUTOSAR controller is in diagnostic mode and waiting for synchronization the scan chains are held in scan mode. Clocking the AUTOSAR controller’s diagnostic clock input causes the scan chain to shift once.

III. SIMULATION RESULTS

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metric packet delivery ratio defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. RO defines the ratio of the amount of routing related transmissions.

Fig. 4 Packet transmission transmitter and receiver

Fig. 5 Packet delivery ratio

IV. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. AUTOSAR protocol specially designed for MANETs is proposed and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK. AUTOSAR techniques to further reduce the network overhead caused by digital signature, and improving the performance metrics.

V. REFERENCES


