IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

EAACK-NEW SECURE INTRUSION DETECTION SYSTEM FOR AD-HOC NETWORK

[#1]G C DIVYA - M.Tech Pursuing,
[#2] KOLLA PALLI RAMESH BABU -Associate Professor,
Department of Computer Science & Engineering,
MALLAREDDY ENGG.COLLEGE FOR WOMEN, Hyderabad.

Abstract: *In recent years mobile ad hoc networks (MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. In this paper, we propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious- behavior-detection rates in certain circumstances while does not greatly affect the network performances.*

Keywords*-- Digital signature, MANET, DSR, AODV.*

I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. However, there is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. 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 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. 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.

1.1 MOBILE ADHOC WIRELESS NETWORK:

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. The rest of this chapter is organized as follows – initially a classification of wireless networks in use today is described followed by the background and origins of adhoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting, applications.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

1.1.1 Classification of Wireless Networks:

A wireless network in general consists of a set of mo-bile hosts which communicate to other mobile hosts either directly or via an access point (base station).The following is a broad classification of wireless networks.

1.1.2 Wireless LANs and PANs

A Wireless Local Area Network (WLAN) consists of a set of mobile users communicating via a fixed base station or an access point. The mobile node can be any de-vice such as a palmtop, PDA, laptop etc.

A Wireless Personal Area Network (WPAN) consists of personal devices which communicate without any established infrastructure. The IEEE 802.15.1 standard for Wireless Personal Area Networks, also called popularly as the Bluetooth is currently being used for short range communication such as in digital cameras, PDAs, lap-tops, etc.

1.1.3 Wireless WANs and MANs

Nowadays, the trend is towards a *wireless internet* consisting of mobile nodes accessing the internet without the help of any backbone network. This type of network is based on the *cellular* architecture in which a large area to be covered is divided in to several cells, each having a fixed base station. Each cell consists of several mobile terminals (MT) which communicate to other mobile terminals in a same cell through the base station as shown in Figure1.2.

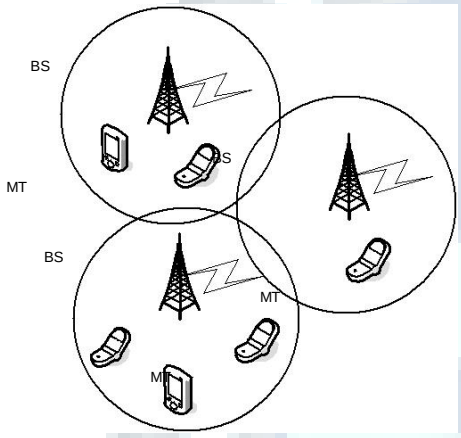

Figure 1.2: A Cellular network

1.1.4 Mobile Ad hoc and Sensor Networks

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations.

They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Fig-ure.1.3, there are no base stations and every node must co-operate in forwarding packets in the network.

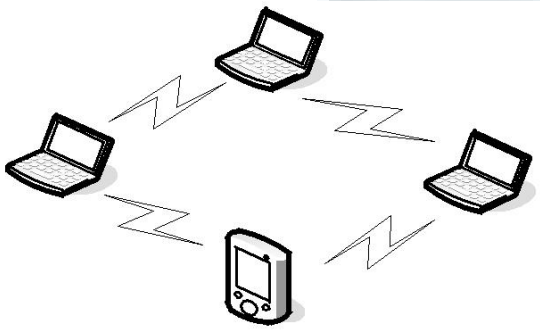

Figure 1.3 MANET

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes

have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care.

1.2 ADVANTAGES OF MOBILE AD HOC NET-WORKS:

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

(a) *Low cost of deployment*: As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

(b) *Fast deployment*: When compared to WLANs, ad hoc networks are very convenient and easy to de-ploy requiring less manual intervention since there are no cables involved.

(c) *Dynamic Configuration:* Ad hoc network configuration can change dynamica ly with time. For the many scenarios such as data sharing in class-rooms, etc., this is a useful feature. When com-pared to configurability of LANs, it is very easy to change the network topology.

EXISTING SYSTEM:

The Watchdog/Path rater is a solution to the problem of selfish (or "misbehaving") nodes in MANET. The system introduces two extensions to the DSR algorithm to mitigate the effects of routing misbehavior the Watchdog, to detect the misbehaving nodes and the Path rater, to respond to the intrusion by isolating the selfish node from the network operation.

Intrusion Detection system in MANETS

As discussed before, 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, Intrusion Detection System (IDS) should be added to enhance the security level of MA-NETs. If MANET can detect the attackers as soon as they enter the network, we will be able to complete-ly eliminate the potential damages caused by compromised nodes at 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, TWOACK and AACK.

WATCHDOG:

Watchdog that aims to improve throughput of net-work with the presence of malicious nodes. In fact, the watchdog scheme is consisted of two parts, namely Watchdog and Pathrater. Watchdog serves as an intrusion detection system for MANETs. It is responsible for detecting malicious nodes misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listens to its next hop's transmission. If Watchdog node overhears that its next node fails to for-ward the packet within a certain period of time, it in-creases its failure counter.

Whenever a node's failure counter exceeds a pre-defined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following researches and implementations have proved that the Watchdog scheme to be efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme.

Watchdog scheme fails to detect malicious misbehaviors with the presence of

ambiguous collisions,
receiver collisions,
limited transmission power, false
misbehavior report, collusion,
partial dropping

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

TWOACK:

TWOACK is neither an enhancement nor a Watch-dog 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).

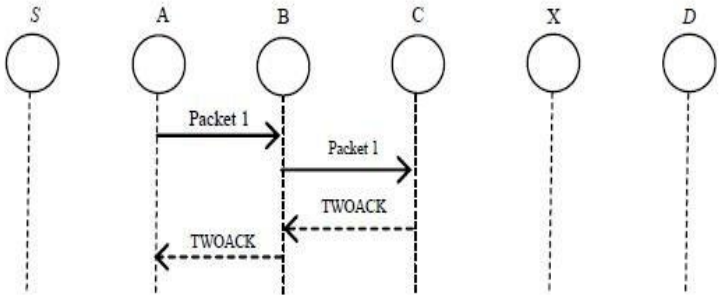

Fig1.4: TWOACK

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 A. 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 a predefined time period, both nodes B and C are re-ported 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 un-wanted network overhead. Due to the limited battery power nature of MANETs, Such redundant transmission process can easily degrade the life span of the entire network.

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.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

II. PROPOED SYSTEM

Proposed System Architecture

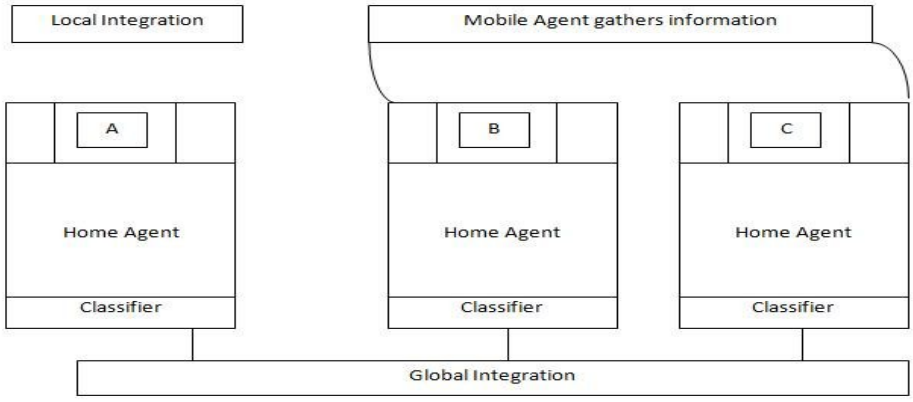

Figure2: Proposed System

Current node: If an attacker sends any packet to gather information or broadcast through this system, the Home-Agent calls the classifier construction to find out the at-tacks. If an attack has been made, it will filter the respective system from the global networks. *Home agent:* is present in each system and it gathers in-formation about its system from application layer to routing layer.

Neighboring node: Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighboring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighboring node.

Data collection: Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the nor-mal scenario. Attack data is collected during the attack scenario.

Data process: The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data preprocess is a technique to process the information with the test train data. In the entire layer anomaly detection systems, the above mentioned preprocessing technique is used. Cross feature analysis for classifier sub model construction.
Local integration: Local integration module concentrate on self system and it find out the local anomaly attacks. Each and every system under hat wireless networks follows the same methodology to provide a secure global network.

Global integration: Global integration module is used to find the intrusion result for entire network. The aim of global integration is to consider the neighbor node(s) result for taking decision towards response module.

III. PROBLEM IDNTIFICATION

My proposed approach EAACK is designed to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and receiver collision. In this section, we discuss these three weaknesses in details. In a typical example of receiver collisions, demonstrated in Fig. 4, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to it tries to node C.; meanwhile, node X is forwarding packet 2 to node C .In such case, node A overheads that node B has successfully, forwarded packet 1 to node C, failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

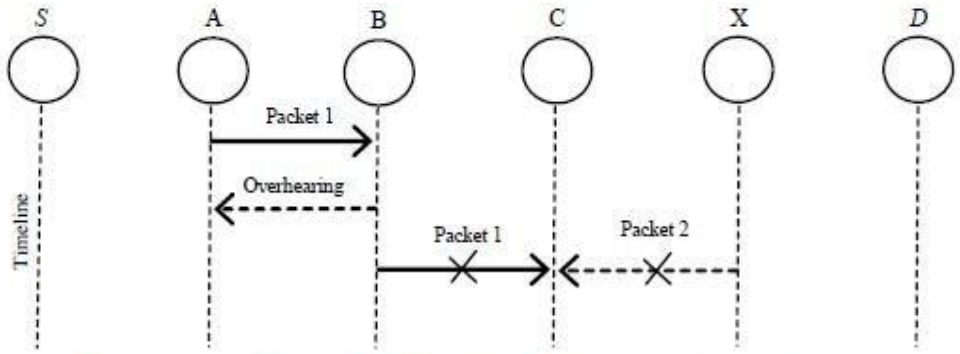

Fig. 4. Receiver Collisions: both node B and node X are trying to send packet 2 to node C at the same time.

In the case of limited transmission power, in order to preserve its own battery resources, node B intentionally limits its transmission power so that it is strong enough to be overheard by node A but not strong enough to be received by node C, as shown in Fig. 5.

For false misbehavior report, although node A successfully overheard that node B forwarded Packet 1 to node C, node A still reported node B as misbehaving as shown in Fig. 6. Due to the open medium and remote distribution of typical MANETs, attackers can easily capture and compromise one or two nodes to achieve this false misbehavior report attack.

As discussed in previous sections, TWOACK and AACK solve two of these three 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 s propose a new intrusion detection system specially designed for MANETs, which solves not only receiver collision and limited transmission power, but also the false misbehavior problem.

IV. SCHEME DESCRIPTION

In this section, we describe our proposed Enhanced Adaptive Acknowledgement (EAACK) scheme in de-tails. The approach described in this research paper is based on our previous work [12], where the backbone of 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.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

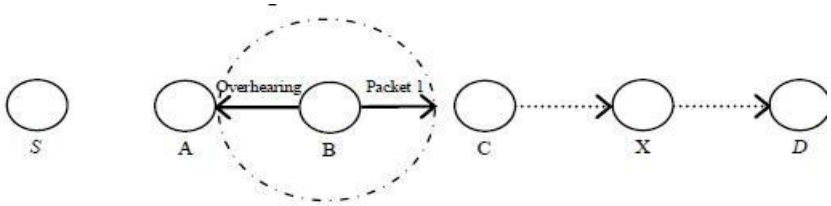

Fig. 5. Limited Transmission Power: node B limits its transmission power so that the packet transmission can be overheard by node A but too weak to reach node C.

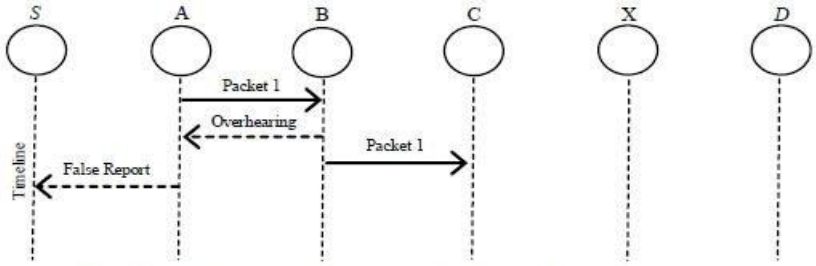

Fig. 6. False Misbehaviour Report: node A send back misbehavior report even though Node B forwarded the packet to node C.

Flowchart describing EAACK scheme. Please note that in my proposed scheme, I assume that the link between each node in the network is bi-directional. Furthermore, for each communication pro-cess, both the source node and the destination node are not malicious. Unless specified, all acknowledgement packets described in this research are required to be digitally signed by its sender and verified by its receiver.

A. ACK

As discussed before, 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. In Fig. 7, in ACK mode, node S first sends out an ACK data packet *ad*1 *P* t o the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node successfully receives *ad*1 *P* , node D is required to send back an ACK acknowledgement packet *ak*1 *P* along the same route but in a reverse order. Within a predefined time period, if node S receives *ak*1 *P* , 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.

B. 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 required to send an S-ACK acknowledgement 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

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 out S-ACK data packet to node F2. Then node F2 forwards this packet to node F3. When node F3 receives, as it is the third node in this three-node group, node F3 is required 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 ad P 1 s ad P 1 s akP 1 s akP

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 in our proposed scheme.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *s ad*1 *P* to node F2. Then node F2 forwards this packet to node F3. When node F3 receives *s ad*1 *P* , as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgement packet*s ak*1 *P* to node F2. Node F2 forwards *s ak*1 *P* 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 in our proposed scheme.

C. 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.

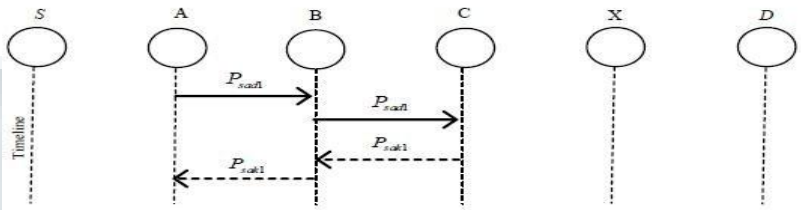

Fig. 8. S-ACK Scheme: node C is required to send back an acknowledgement packet to node A.

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.

To initiate MRA mode, the source node first searches its local knowledge base and seeks for alternative route to the destination node. If there is none other exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes.

By adopting an alternative route to the destination node, we circumvent the misbehavior reporter node. 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.

By the adoption of MRA scheme, EAACK is capable of detecting malicious nodes despite the existence of false misbehavior report.

D. Digital Signature

As discussed before, EAACK is an acknowledgement based IDS. All three parts of EAACK, namely: ACK, S-ACK 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 en-sure 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.

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 type of attacks, we propose three scenario settings to simulate different type of misbehaviors or attacks.

1) 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) 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.

3) 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.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC-4.3 and Ubuntu 9.10. The system is running on a laptop with Core 2 Duo T7250 CPU and 3GB RAM.

In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. The intention is to provide more general results and make it easier for us to compare the results. In NS 2.34, the default configuration specifies 50 nodes in a flat space with the size of 670x670m. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the wireless extension of NS2.

The moving speed of mobile node is limited to 20m/s and a pause time of 1000s. UDP traffic with Constant Bit Rate (CBR) is implemented with a packet size of 512 bytes.

For each schemes, we ran every network scenarios for three times and calculated the average performance. In order to measure and compare the performance of our proposed scheme, we continue to adopt the following two performance metrics:

Packet Delivery Ratio (PDR):- PDR defines the ratio of the number of packets received by the destination node and the number of packets sent by the source node.

Routing Overhead (RO):- RO defines the ratio of the amount of routing-related transmissions (RREQ, RREP, RERR, ACK, S-ACK and MRA).

During the simulation, the source route broadcasts a Route REQuest (RREQ) message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcast this new message to their neighbors.

If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in flat routing protocols like DSR, a Route ERR or (RERR) message is sent to the source node. When the RREQ message arrives to its final destination node, the destination node initiates a Route REPly (RREP) message and sends this message back to the source node by reversing the route in the RREQ message.

Regarding the digital signature schemes, we adopted an open source library named Botan. This cryptography library is locally compiled with GCC 4.3. To com-pare performances between DSA and RSA scheme, we generated 1024 bit DSA key and 1024 bit RSA key for every node in the network.

We assumed that both a public key and a private key are generated for each node and they were all distributed in advance. Typical size of public key and private key file is 654 bytes and 509 bytes with a 1024 bit DSA key respectfully. On the other hand, the size of public key and private key file for 1024 RSA is 272 bytes and 916 bytes respectively. The signature file size for DSA and RSA is 89 bytes versus 131 bytes respectively.

In terms of computational complexity and memory consumption, we did a research on popular mobile sensors. According to our research, one of the most popular sensor nodes in the market is Tmote Sky. This type of sensor is equipped with a TI MSP430F1611 8MHZ CPU and 1070KB of memory space. We believe this is enough for handling our simulation settings in terms of both computational power and memory space.

IPHV7I20042X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .II
ISSN Online: 2319 – 9253
Print: 2319 – 9245

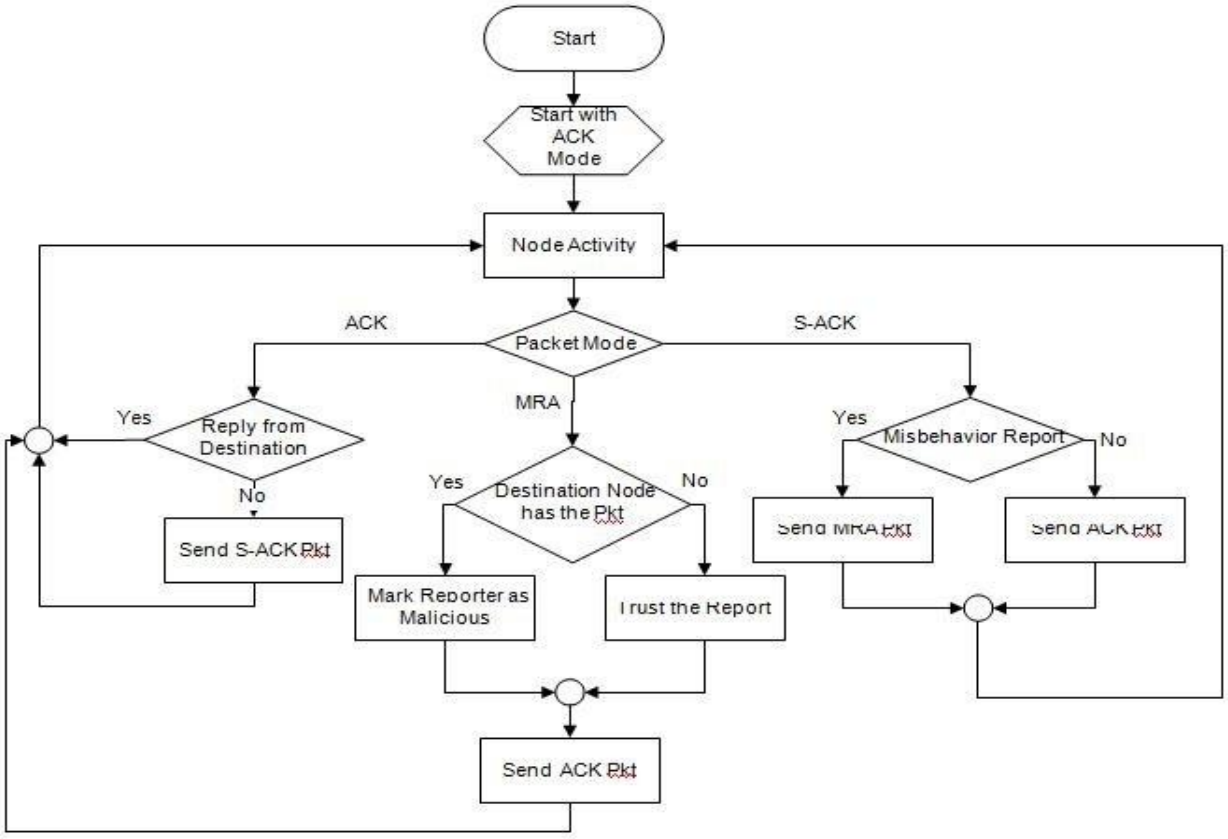

Fig: 7 System flow of EAAC

VI. CONCLUSION AND FUTURE WORK

Packet-dropping attack has always been a major threat to the security in MANETs. In this research paper, we have proposed a novel 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, we extended our research 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. We think that this tradeoff is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits of our research work, we plan to investigate the following issues in our future research:

REFERENCES

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

[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 – here1

[3] R.H. Akbani, S. Patel, D.C. Jinwala. "DoS Attacks in Mobile AdHoc Networks: A Survey", the proceedings of the Second Interna-tional Meeting of Advanced Computing & Communication Tech-nologies (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] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and Optimization of a Solar Energy Harvester System for Self-Powered Wireless Sensor Networks," IEEE Trans. on In-dustrial Electronics, vol. 55, no. 7, pp. 2759-2766, July 2008.

[7] V. C. Gungor, G. P. Hancke, "Industrial Wireless Sensor Net-works: Challenges, Design Principles, and Technical Approac," IEEE Trans. on Industrial Electronics,

vol. 56, no. 10, pp. 4258-4265, Oct 2009.

[8] Y. Hu, D. Johnson and A. Perrig. SEAD: Secure Efficient Dis-tance Vector Routing for Mobile Wireless Ad Hoc Networks. In the Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, 2002.

[9] Y. Hu, A. Perrig, and D. Johnson. ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks. In the Proceed- ings of the 8th ACM International Conference on Mobile Compu-ting and Networking (MobiCom'02), pp. 12-23, Atlanta, GA,2002.

[10] G. Jayakumar and G. Gopinath. Ad Hoc Mobile Wireless Net-works Routing Protocol – A Review. In Journal of Computer Sci-ence 3(8): 574-582, 2007.

[11] D. Johnson and D. Maltz. Dynamic Source Routing in Ad hoc Wireless Networks. Mobile Computing, Kluwer Academic Pub-lishers, Chapter 5, pp. 153-181, 1996.

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

[13] N. Kang, E. Shakshuki andT. Sheltami. Detecting Forged Acknowledgements in MANETs. The 25th International Confer-ence on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore, March 22-25, 2011.

[14] K. Kuladinith, A.s Timm-Giel and C. Görg. Mobile Ad-Hoc Communications in AEC industry. In Journal of Information Technology in Construction Vol. 9, pp. 313-323, 2004.

[15] Jin-Shyan Lee, "A Petri Net Design of Command Filters for Sem-iautonomous Mobile Sensor Networks," IEEE Trans. on Industrial Electronics, vol. 55, no. 4, pp. 1835-1841, April 2008.

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

[17] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehaviour in Mobile Ad hoc Networks. In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.

[18] A. Menezes, P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography, CRC Press, T-37, 1996.

[19] N. Nasser and Y. Chen. Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network, In Proceedings of IEEE International Conference On Communica-tion, Glasgow, Scotland, June 24 – 28, 2007.

[20] J. Parker, J. Undercoffer, J. Pinkston and A. Joshi. On Intrusion Detection and Response for Mobile Ad hoc Networks. In the Pro-ceedings of IEEE International Conference on Performance, Computing, and Communications, pp. 747-752, 2004

[21] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. In the Commu-nications of ACM, vol. 21, pp. 120-126, 1978.

[22] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, S. Lan-ceros-Mendez, "Energy Harvesting From Piezoelectric Materials Fully Integrated in Footw," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 813-819, March 2010.

[23] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, 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.

[24] A. Singh, M. Maheshwari and N. Kumar. "Security and Trust Management in MANET", in Communications in Computer and Information Science, vol. 147, part 3, pp. 384-387. Springer, 2011
– here1

[25] B. Sun. Intrusion Detection in Mobile Ad hoc Networks. Doctoral Dissertation. Texas A&M University, 2004.

AUTHOR'S PROFILE:

[1]. G C DIVYA, Pursuing M.Tech in Department of Computer Science & Engineering at Malla Reddy Engg.College For Women, Hyderabad,Telangana,India.

[2]. KOLLA PALLI RAMESH BABU, working as Associate .Professor in Department of Computer Science & Engineering at Malla Reddy Engg.College For Women, Hyderabad,Telangana,India.