The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 9 ||Pages|| 32-40||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme In Receiver Collisions – An IDS In Wireless Mobile Ad-Hoc Networks

[1,] S. Sujatha, [2,] B. Lakshmi Radhika

[1,] Associate Professor MCA,Mphil (cs),(PhD)School Of IT&Science, Dr.G.R.Damodaran college of science Coimbatore

[2,] M.Phil(CS) Research Scholar, School Of IT & Science, Dr.G.R.Damodaran college of science Coimbatore

--ABSTRACT---

MANET is a collection of wireless mobile nodes forming a network without using any existing infrastructure. There are various challenges that are faced in the Ad-hoc environment. These are mostly due to the lack of resources of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. This paper focuses on the comparative study of handling receiver collisions in watch dog using Enhanced Adaptive Acknowledge (EAACK). The key issues concerning these areas have been addressed here. The main focus has been laid on study of EAACK approach and its limitation.

KEYWORDS *: AACK, EAACK, MANET, Receiver Collision, Watch Dog*

Date of Submission: 29,August, 2013 Date of Acceptance: 20, September 2013

I. INTRODUCTION

In a mobile ad hoc network (MANET), a collection of mobile hosts with wireless network interfaces to form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In other words a MANET is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed, this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. In a MANET, nodes within each other’s wireless transmission ranges can communicate directly; however, nodes outside each other’s range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Every node functions as a router. The success of communication highly depends on other nodes cooperation.

1.1 MOBILE ADHOC WIRELESS NETWORK:

The Mobile Ad hoc Wireless Network is more vulnerable to be attacked than wired network. These vulnerabilities are nature of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised *to exploit* these vulnerabilities and *to cripple* the MANET operation. 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 ad hoc wireless networks. The general issues in ad hoc wireless networks are then discussed, followed by a few interesting applications. The final section gives an outline of the chapters to follow.

Fig 1.1Wireless MANET

1.1.1 Taxonomy of Wireless Networks

A wireless network in general consists of a set of mobile 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 device 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, laptops, 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.

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. There are no base stations and every node must co-operate in forwarding packets in the network. 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.

1.2 ADVANTAGES OF MOBILE AD HOC NETWORKS:

(a) Low cost of deployment: As the name suggests, adhoc 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, adhoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

(c) 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.

1.3 EXISTING SYSTEM:

1.3.1 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 address this problem, Intrusion Detection System (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 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 the existing approach, namely, the Watchdog to detect the misbehaving nodes.Watchdog aims to improve throughput of network 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 listening 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 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.

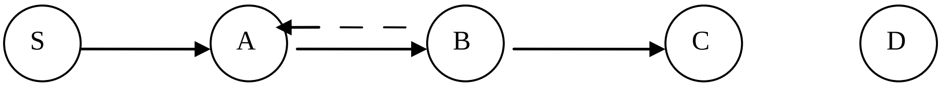


Fig 1.3.2 Operation of the watchdog.

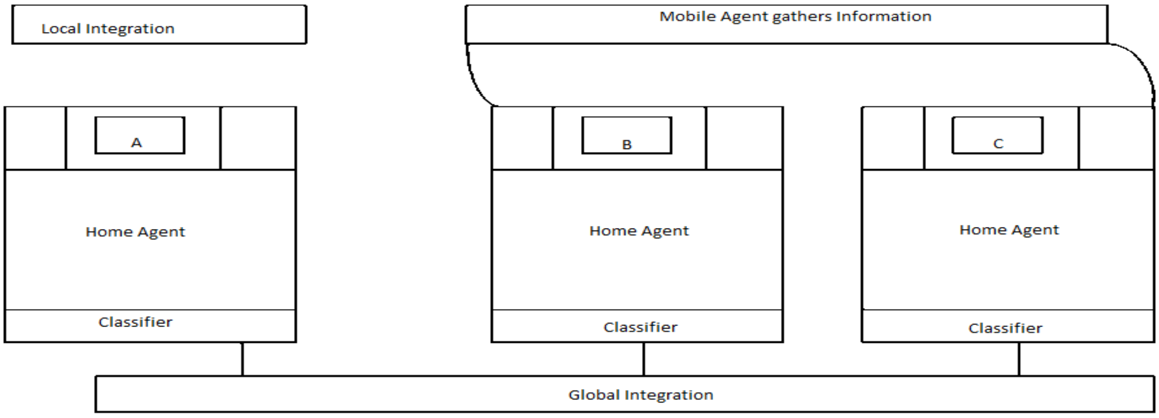
Figure 1.3.2 illustrates the operation of the watchdog. Node A cannot transmit all the way to node C, but it can listen to node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the headers We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

1.3.3 Limitations of Watchdog

The watchdog mechanism can detect misbehaving nodes at forwarding level and not at the link level. Watchdog scheme fails to detect malicious misbehaviors with the presence of

- ambiguous collisions,
- receiver collisions,
- limited transmission power,
- false misbehavior report,
- collusion
- partialdropping.

1.3.4 Existing 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 attacks. If an attack has been made, it will filter the respective system from the global networks.

Home agent: It is present in each system and it gathers information 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 normal 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.

II. PROPOSED SYSTEM

My proposed approach is to study in detail of the TWOACK and AACK designed to tackle one of the six weaknesses of Watchdog scheme, namely receiver collisions. In this section, we discuss the weakness in detail.

2.1 Receiver collision

In the receiver collision problem as illustrated in the figure 2.1the node A can only identify whether node B has sent the packet to node C, but node A cannot assure that node C has received it. If a collision occurs at node C when node B first forwards the packet, node A can only assume that node B has forwarded the packet and assumes that node C has successfully received it. Thus, B could skip retransmitting the packet and evade detection.

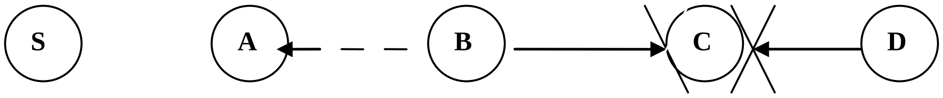


Fig 2.1 Receiver Collision.

In a typical example of receiver collisions, demonstrated in Fig. 2.2, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding packet 2 to node C. In such case, node A overhears that node B has successfully, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between Packet 1 and Packet 2 at node C.

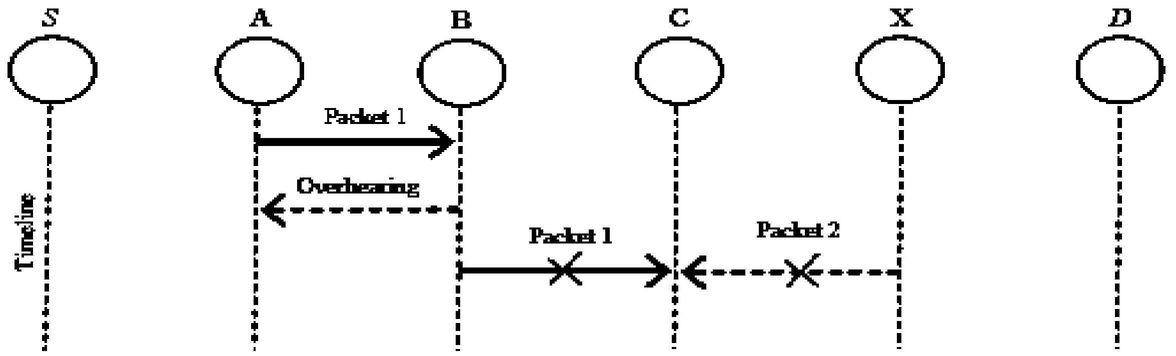


Fig 2.2 Receiver Collisions: both node B and node X are trying to send packets to node C at the same time

An ideal intrusion detection model in MANET should first have a reliable, distributed, low-overhead, message collecting, and exchanging mechanism. The mechanism should also adapt to changes in the network topology and tolerate message loss. Secondly, the model should be affordable for low computation power devices. Third, the model should perform real-time protections since the routing topology may change very quickly and the attack damage may also propagate relatively quickly. Finally, the model should not generate high false positives and negatives with respect to new routing attacks. Intrusion detection is defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource”. [3] Intrusion detection system (IDS) is a practical approach to enhance the security of existing networks. Briefly, an intrusion detection system monitors activity in a system or network in order to identify, to detect, and then to isolate current attacks.

There are three main components of IDS:

- Collection of data.
- Analysis of collected data (Detection).
- Response of an alert when a threat is detected.

For Mobile Ad hoc Networks, the general function of an IDS is detecting misbehaviors by observing the networks traffic in a Mobile Ad hoc [4]. Most of recent researches focused on providing preventive schemes to secure routing in MANETs. In this research we focus on analyzing the previous TWOACK and AACK method and intensively study the limitations of this system.

III. PROBLEM IDENTIFICATION

3.1 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).

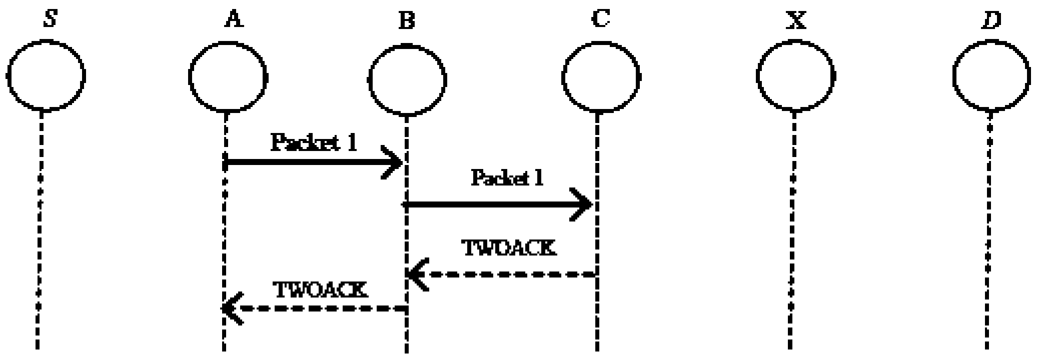


Fig.3.1 TWOACK

The working process of TWOACK is demonstrated in Fig. 3.1, 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 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 network.

3.2 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 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 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, the approach described in this research paper is based on our previous work [1], [2], where the backbone of EAACK was proposed and evaluated through implementation. In this work, we analyze the digital signature which has been proposed in our previous work [2] to prevent the attacker from forging acknowledgement packets. We analyze the EAACK scheme and study the limitations of this scheme.

IV. SCHEME DESCRIPTION

The previous approach EAACK is designed to tackle three of the six weaknesses of Watchdog Scheme, namely false misbehavior [2], limited transmission power [2] and receiver collision [2]. In this section, we discuss one of these three weaknesses namely Receiver Collisions in detail. In a typical example of receiver collisions, demonstrated in Fig. 4.1, after node A sends Packet 1 to node B, it tries to overhear if node B forwarded this packet to node C; meanwhile, node X is forwarding Packet 2 to node C. In such case, node A overhears that node B has successfully, forwarded Packet 1 to node C, but failed to detect that node C did not receive this packet due to a collision between
Packet 1 and Packet 2 at node C.

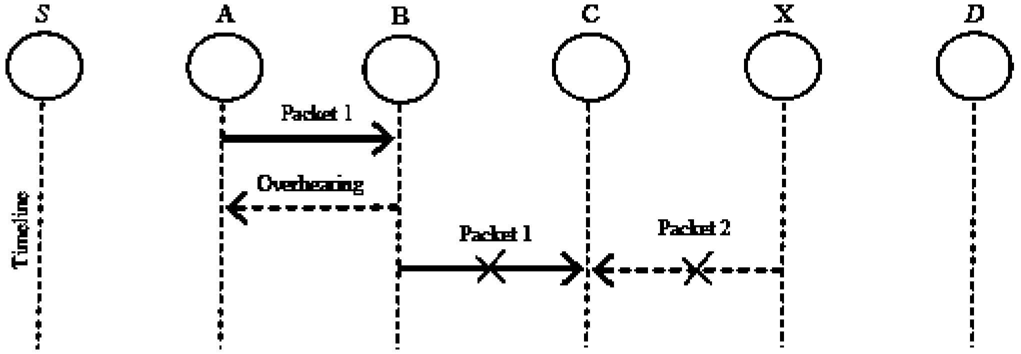


Fig. 4.1 Receiver Collisions: both node B and node X are trying to send packet 2 to node C at the same time

As discussed in previous sections, TWOACK and AACK solve two of these three weaknesses, namely receiver collision and limited transmission power [2]. 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 [2] work the EEACK 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. EAACK was proposed and evaluated through implementation. In the previous work [2] the EAACK scheme was extended 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, they included a two-bit packet header in EAACK. According to the Internet draft of DSR [11], there are six bits reserved in DSR header. In EAACK, two of the six bits were used to flag different type of packets. In the proposed scheme [2] it was assumed that the link between each node in the network is bi-directional. Furthermore, for each communication process, 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 [1]. We briefly describe the three major parts of EAACK [2].A. 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. In ACK mode, node S first sends out an ACK data packet ad1 P to the destination node D. If all the intermediate nodes along the route between node S and node D are cooperative and node D successfully receives ad1 P, node D is required to send back an ACK acknowledgement packet ak1 P along the same route but in a reverse order. Within a predefined time period, if node S receives ak1 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. [15]. 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. 4.1, 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 packet 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 reported as malicious. Moreover, a misbehavior report will be generated by node F1 and sent to the source node S. 1 s adP 1 s adP 1 s akP 1 s akP. 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.

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.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 report 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

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, [1] incorporated digital signature in their 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.

V. CONCLUSION

However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, [1] implemented both DSA [13] and RSA [14] digital signature scheme in their proposed approach. The goal was to find the most optimal solution for using digital signature in MANETs. Digital signature algorithms are used to provide authentication of data and validating the sender. Algorithms discussed include the signature algorithms RSA and DSA. The DSA algorithm has the limiting factor that only the owner of the private key can create the digital signature hence it can be used to verify who created a message and anyone knowing the public key can verify the signature provided they are confident of the identity of the owner of the public key.With DSA, the entropy, secrecy, and uniqueness of the random signature value k is critical. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping k secret), using a predictable value, or leaking even a few bits of k in each of several signatures, is enough to break DSA. Every RSA initialization process requires the random selection of two very large primes, traditionally referred to as p and q, and computing n such that n=pq. Previously, we extolled the virtues of RSA over DSA, citing that RSA could be used for encryption and digital signature applications, while DSA was strictly for digital signature applications. In the real world, the encryption capabilities of RSA are rarely used for one simple reason: the length of the plaintext that can be encrypted is limited to the size of n. In fact, the real length is even smaller than n because of the overhead introduced by the algorithms. As a result, the pre dominate approach is to generate a random secret key and encrypt that key with the RSA keys. The message is then encrypted using a symmetric cipher with the generated secret key. With these limitations the EAACK [1] approach needs to be further optimized for the digital signature schemes.

REFERENCES

[1] U. Sharmila Begam, Dr. G. Murugaboopathi - A Recent Secure Intrusion Detection System for MANETs, International Journal of Emerging Technology and Advanced Engineering, Volume 3, Special Issue 1, January 2013 – here 1

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

[3] 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 – here 2

[4] R.H. Akbani, S. Patel, D.C. Jinwala. “DoS Attacks in Mobile Ad Hoc Networks: A Survey”, the proceedings of the Second International Meeting of Advanced Computing & Communication Technologies (ACCT) , pp. 535-541, Rohtak, Haryana, India. 2012. – here 2

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

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

[7] 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 – here 2

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

[9] K. Stanoevska-Slabeva and M. Heitmann. Impact of Mobile Ad- Hoc Networks on the Mobile Value System. 2nd Conference on m-Business, Vienna, June 2003.

[10] A. Tabesh, L. G. Frechette, "A Low-Power Stand-Alone Adaptive Circuit for Harvesting Energy From a Piezoelectric Micropower Genera," IEEE Trans. on Industrial Electronics, vol. 57, no. 3, pp. 840-849, March 2010.

[11] M. Zapata and N. Asokan. Securing Ad hoc Routing Protocols. In the ACM Workshop on Wireless Security, pp. 1-10, 2002.

[12] L. Zhou and Z. Haas. Securing Ad-hoc Networks. In the IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, 1999.

[13] Digital Signature Standard (DSS). Federal Information Processing Standards Publication, National Institute of Standards and Technology, Gaithersburg, MD, 2009.

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

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

AUTHORS PROFILE

S. Sujatha completed her undergraduate degree at Sri Sarada College for Women, Tirunelveli and has also completed post graduate level courses MCA and MPhil at Bharathiar University, Coimbatore, India, and is currently pursuing her doctorate in Computer Science. Her area of interest is Mobile Agent Technology & Networks. She has been participating continuously in research and development activities for the past ten years. To her credit, she has presented and published technical papers in International Journals, at International Conferences and International Workshops organized by various international bodies like IEEE, WSEAS, and IEEE Explore. She has published book on Integrating SOA and Web Services and also contributed chapters on Personal Area Network and published articles & working manuals in agent technology. The author is currently employed as Associate Professor at the Dr. G.R Damodaran College of Science, Coimbatore, India. She is an active member of various technical bodies like ECMA, Internet Society of Kolkata and Chennai and acts as a moderator in various international conferences and journals.

B. Lakshmi Radhika completed her undergraduate degree at NGM college, Pollachi and has also completed her post graduate level course MCA at Bharadhidasan University, Tiruchirapalli, and is currently pursuing her Mphil in Computer Science at Dr. G.R Damodaran College of Science, Coimbatore, India. Her area of interest is Advanced Networking.