ISSN:0975-9646

New Secure Intrusion-Detection System for Manet's Using Hybrid Cryptography Techniques

E.Malini[1], T.Ravi[2]

[1]Assistant Professor, [2]Post Graduate Scholar
Department of Computer Science
Arulmigu Meenakshi Amman College of Engineering
Namandi Post, Vadamavandal. 604410

***Abstract*-The technology change in wireless from wired has been a comprehensive trend in the past few years. The mobility and scalability brought by wireless network prepared it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETworks (MANET) is one of the most vital and exclusive applications. On the contrary to traditional network architecture, MANET does not need a stable network infrastructure; the self-configuring ability of nodes in MANET made it popular among critical mission application like military use or emergency retrieval. However, the open medium and wide sharing of node make MANET vulnerable to malicious attackers. Hear crucial to develop capable intrusion-detection mechanisms to guard MANET from attacks. With the enhancements of the technology and changed in hardware costs, we are watching a current trend of expanding MANETs into industrial applications. To propose and implement a new intrusion-detection specially designed for MANETs. Compared to contemporary approaches, new intrusion-detection system demonstrates higher malicious-behaviour-detection rates in certain conditions while does not greatly affect the network performances.**

Index Term: **Digital Signature, New Intrusion Detection, Mobile Ad Hoc Network (MANET)**

I. INTRODUCTION

A new Intrusion-Detection system technique is used to avoid a malicious node in the MANETS, the malicious attacker used the wide delivery and open medium features of the MANETS to establish the vulnerabilities in the network. The recent years, the explosive growth of mobile computing devices, which primarily include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a innovative change in the computing world: computing will not merely have faith in the capability provided by the personal computers, and the concept of global computing arises and becomes one of the study hotspots in the computer science society. The nature of the ubiquitous computing has made it required to adopt wireless network as the interconnection method: it is not possible for the pervasive devices to get wired network link whenever and wherever they need to connect with other pervasive devices.

The Mobile Ad Hoc network is one of the wireless networks that have involved most applications from many investigators. MANET is a self-configuring infrastructure network of mobile devices associated by wireless network it equipped with both a wireless transmitter and a receiver that interconnect each other bidirectional wireless either directly or indirectly. One of the main advantages of wireless networks is its ability to allow data communication among different parties and still maintain their mobility. This means that two nodes can't interconnect with each other when the space among the two nodes is outside the communication range of their own.

MANET resolves this problem by permitting midway parties to relay data communications. This is achieved by dividing. MANET into two types of networks, namely, single-hop and multi hop. Unluckily, the open medium and distant distribution of MANET make it helpless to various types of attacks. Due to the nodes lack of physical protection, malevolent attackers can easily capture and compromise nodes to realize attacks. In particular, seeing the fact that most routing protocols in MANETs assume that every node in the network behaves helpfully with other nodes and presumably not malicious. If MANET can sense the attackers as soon as they arrive the network, we will be able to completely remove 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. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected thru wireless. Each device in a MANET is free to move independently in any way, and will therefore change its links to other devices recurrently. Each must forward traffic unconnected to its own use, and therefore be a router. The major challenge in building a MANET is equipping each device to endlessly maintain the information required to properly route traffic. Such networks may function by themselves or may be linked to the larger Internet. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies.

The mobile ad hoc network, nodes can straight communicate with all the other nodes inside their radio ranges; whereas nodes that not in the straight communication range use midway node(s) to communicate with each other. In these two states, all the nodes that have contributed in the communication automatically form a wireless network, therefore this kind of wireless network can be observed as mobile ad hoc network. The mobile ad hoc network has the following typical features:

i. Undependability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links

between mobile nodes in the ad hoc network are not steady for the communication members.

ii. Constantly altering topology. Due to the nonstop wave of nodes, the topology of the mobile ad hoc network changes always, the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing data will be varying all the time because of the movement of the nodes.

iii. Lack of incorporation of safety features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing always, it is needed for each pair of nearby nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of weaknesses in the statically configured routing protocol.

II. IDS IN MANETS

Due to the limits of most MANET routing protocols, nodes in MANETs assume that other nodes always co-operate with each other to relay data. This guess leaves the attackers with the openings 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 safety level of MANETs. If MANET can detect the attackers as soon as they enter the network, we will be able to completely remove the possible 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. In this section, we mainly label three existing tactics, specifically, Watchdog, TWOACK, and Adaptive ACKnowledgment (AACK).

A. WATCH DOG

The proposed a scheme named Watchdog that aims to advance the throughput of network with the occurrence of malicious nodes. In fact, the Watchdog scheme is involved of two parts, namely, Watchdog and Path ratter. Watchdog serves as IDS for MANETs. It is answerable for discovering malicious node misbehaviors in the network. Watchdog identifies malicious misbehaviors by wantonly listening to its next hop's transmission. If a Watchdog scheme node overhears that its next node fails to forward the packet within a sure period of time, it raises its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog scheme node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Many of succeeding research studies and implementations has proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is skilled of discovering malicious nodes rather than links. These advantages have made the Watchdog scheme a prevalent choice in the field.

The Watchdog scheme miss the mark to detect malicious misbehaviors with the presence of the following: 1) Ambiguous collisions 2) Receiver collisions, 3) Limited transmission power, 4) False misbehavior report, 5) Collusion, 6) Partial dropping.

B. TWOACK

With respect to the six faults of the Watchdog scheme, many researchers planned new methodologies to solve these issues. TWOACK proposed by K.Liu [5] is one of the most important approaches among them. On Figure.2.1. TWOACK scheme: Each node is required to send back an acknowledgment packet to the node that is two hops left from it. The contrary too many other schemes, TWOACK is neither an enhancement nor a Watchdog-based system. Take aim to resolve the receiver collision and limited broadcast power problems of Watchdog, TWOACK senses misbehaving links by acknowledging every data packet conveyed over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is necessary to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK [3] is required to work on routing protocols such as Dynamic Source Routing (DSR). The working process of TWOACK is shown in Figure.2.1. TWOACK scheme

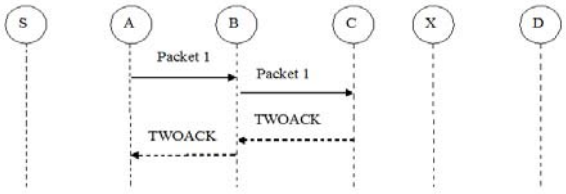


Figure.2.1. TWOACK Scheme

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 left from node A, node C is pleased to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The rescue of this TWOACK packet at node A indicates that the broadcast 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. The same process applies to every three sequential nodes along the rest of the route. The TWOACK scheme effectively solves the receiver collision and limited broadcast power problems posed by Watchdog. However, the acknowledgment process required in every packet broadcast process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant broadcast process can easily degrade the life span of the entire network. However, many investigation studies are working in energy harvesting to deal with this problem.

C. AACK

Based on TWOACK to suggest a new scheme called AACK. Like to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a blend of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Associated to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The end-to-end acknowledgment scheme in ACK is shown in Figure.2.2.

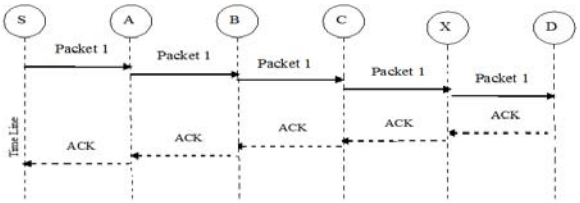


Figure.2.2. ACK Scheme

In the ACK scheme shown in Figure.2.2, the source node S sends out Packet 1 without any overhead. All the midway 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 broadcast 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 [2] importantly decreases the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to sense malicious nodes with the attendance of false misbehavior report and forged acknowledgment packets. In fact, many of the existing IDSs in MANETs adopt an acknowledgment-based scheme, including TWOACK and AACK. The functions of such detection schemes all fundamentally depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are effective and authentic. To speech this concern, we adopt a digital signature in our proposed scheme named new intrusion-detection system.

III. SCHEME DESCRIPTION

In this section, describe our proposed EAACK scheme in detail. The approach described in this research work is based on our previous work, where the backbone of new intrusion-detection system [3] was proposed and evaluated through implementation. New intrusion-detection is involved of three major parts, specifically, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

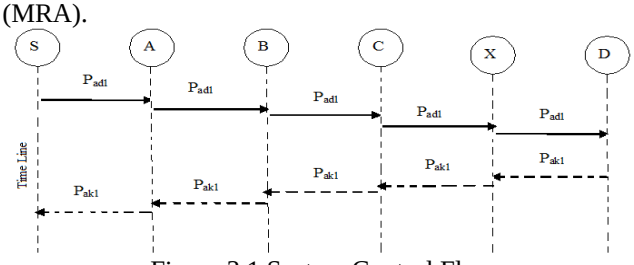


Figure.3.1.System Control Flow

Figure.3.1. presents a flowchart describing the new intrusion-detection system scheme. Please note that, in our proposed scheme, assume that the link among each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets defined in this study are necessary to be digitally signed by its sender and confirmed by its receiver.

3.1. ACK

As discussed before, ACK is fundamentally an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in intrusion detection, aiming to reduce network overhead when no network misbehavior is detected. In Figure.3.2, in ACK mode, node S first sends an ACK data packet P_{ad1} to the destination node D. If all the midway nodes along the route between nodes S and D are cooperative and node D successfully receives P_{ad1}, node D is required to send back an ACK acknowledgment packet P_{ad1} along the same route but in a reverse order. Within a predefined time period, if node S receives P_{ad1}, then the packet broadcast from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending an S-ACK [1] data packet to detect the misbehaving nodes in the route.

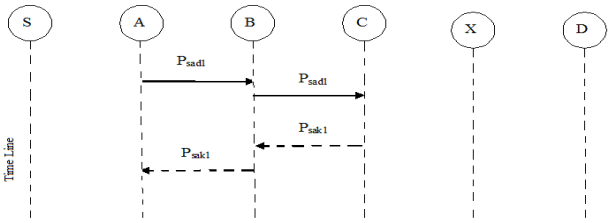


Figure.3.2.ACK Scheme

3.2. S-ACK

The S-ACK [1] scheme is an improved version of the TWOACK scheme proposed by K.Liu. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three serial nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The purpose of presenting S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. As shown in Figure.3.3, in S-ACK mode, the three consecutive nodes (A, B, and C) work in a group to detect misbehaving nodes present in the network. Node A first sends out S-ACK data packet P_{sad1} to node B. Then, node B forwards this packet to node C.

When node C receives P_{sad1}, as it is the third node in this three-node group, node C is necessary to send back an S-ACK acknowledgment packet P_{sak1} to node B. Node B forwards P_{sak1} back to node A. If node A does not receive this acknowledgment packet within a predefined time period, both nodes B and C are reported as malicious. Moreover, a misbehavior report will be generated by node A and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, new intrusion-detection 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.

3.3. MRA

The MRA scheme is designed to resolve the fault of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be produced by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down adequate nodes and thus cause a network division.

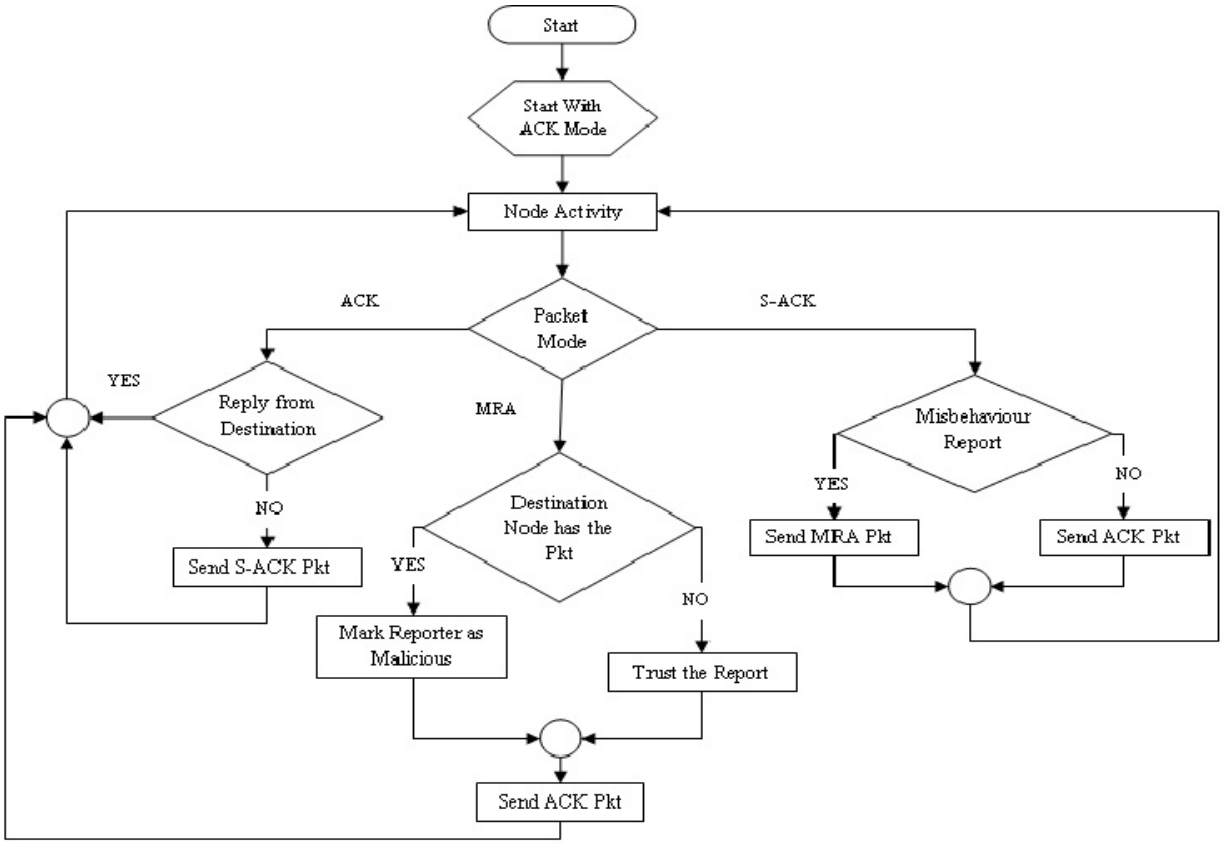


Figure.3.3.S-ACK Scheme

The core of MRA scheme is to validate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node.

The nature of MANETs, it is common to find out multiple routes between two nodes. By adopting an alternative route to the destination node, circumvent the misbehavior reporter node. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received. If it is already received, then it is safe to conclude that 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, new intrusion-detection system is skilled of detecting malicious nodes despite the existence of false misbehavior report.

IV. PROBLEMATIC DEFINITION

My proposed approach new intrusion-detection system is planned to tackle three of the six weaknesses of Watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this section, discuss these three weaknesses in detail In a typical example of receiver collisions, shown in Figure.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 among Packet 1 and Packet 2 at node C.

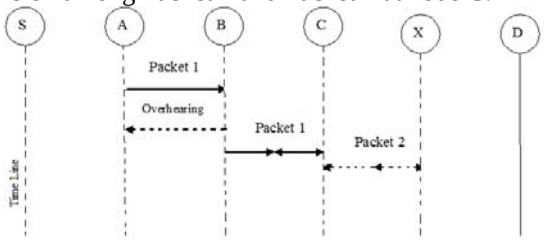


Figure.4.1.Receiver Collisions.

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 Figure.4.2.

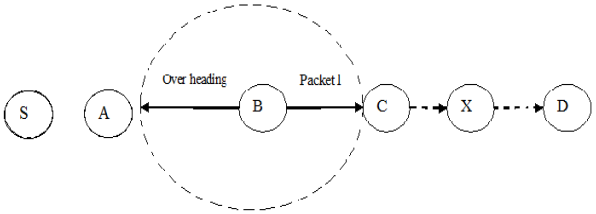


Figure.4.2. Limited Transmission Power

For false misbehavior report [4], 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 Figure.4.3. 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.

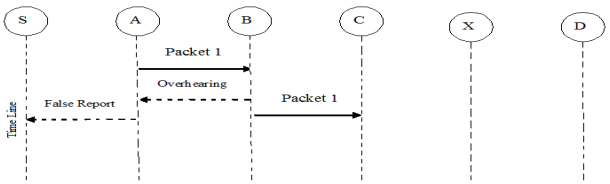
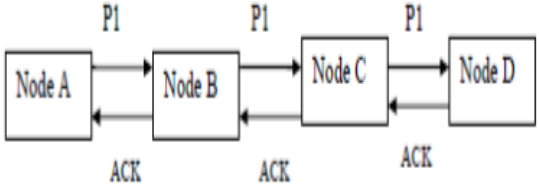


Figure.4.3. False Misbehavior Report

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 propose new IDS specially designed for MANETs [4], which solves not only receiver collision and limited transmission power but also the false misbehavior problem. Furthermore, extend our research to adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is vital to ensure the integrity and authenticity of all acknowledgment packets.

4.1. ACK IMPLEMENTATION

ACK is basically an end – to – end acknowledgment scheme. It is a part of the hybrid new intrusion-detection scheme aiming to reduce the network overhead when no network misbehaviour is detected. The basic flow is if Node A sends a packet p1 to destination Node D, if the entire intermediate nodes are cooperative and effectively receives the request in the Node D.



Figuer.4.4. Node Activity

If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives Pad1, node D is required to send back an ACK acknowledgment packet Pak1 along 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. It will send an ACK to the source (Node A). If ACK from the destination get delayed then it S-ACK process will be initialized.

4.2. SECURE ACKNOWLEDGMENT(S-ACK)

In the S-ACK principle is to let every three consecutive nodes work in a group to sense misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

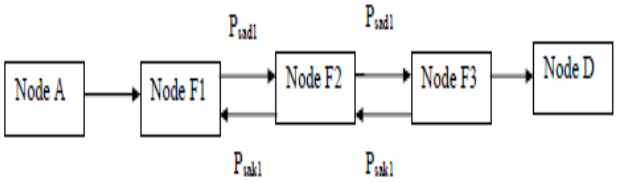


Figure.4.5. S-ACK Implementation

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 Psad1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives Psad1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK [1] acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be produced by node F1 and sent to the source node S. Nevertheless, unlike the TWOACK scheme, where the source node immediately trusts the misbehaviour report, new intrusion-detection 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.

4.3. MISBEHAVIOR REPORT AUTHENTICATION (MRA)

The MRA scheme is calculated to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

V. DIGITAL SIGNATURE VALIDATION

In all the three parts of New Intrusion-Detection, namely, ACK, S-ACK, and MRA [1], are acknowledgment-based detection schemes that all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in new intrusion-detection system are authentic and untainted. Otherwise, if the attackers are smart sufficient to forge acknowledgment packets, all of the three schemes will be vulnerable. There are three algorithms that are suitable for digital signature generation under the DSS standard. They are the Digital Signature Algorithm (DSA, which I will talk about more in depth later), the RSA algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA). Also in this standard is a hash function to be used in the signature generation process. It is used to obtain a condensed version of the data, which is called a message digest. This message digest is then put into the digital

signature algorithm to generate the digitally signed message. The same hash function is used in the verification process as well. The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA).

VI. CONCLUSION

In this research work, I have proposed a novel IDS named new intrusion-detection system protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios java programming. The results established progressive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehaviour 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.

VII. FUTURE WORK

It is proposed for a novel IDS named new intrusion-detection system protocol specially designed for MANETs and, to develop real-time application for wireless devices such as mobile, laptop and tablet etc. using java platform

REFERENCES

1. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE "EAACK—A Secure Intrusion-Detection System for MANETs" IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013
2. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
3. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
4. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
5. K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput. vol. 6, no. 5, pp. 536–550, May 2007.

AUTHORS

E.MALINI, M.E., AP/CSE
E.Mail ID: malinijoy@rediffmail.com
Ph. No: 9994857006
Department of computer science AMACE

T.RAVI is at present pursuing master's degree program in computer science engineering at AMACE.
Ph. No: 9677475655.
Email ID: ravime16@gmail.com.