IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Prevention against Attacks in MANET Using Secure IDS

Darshana Salvi[1], Ruchira Samant[2], Ashwini Patil[3], Manali Repale[4], Prof. Manisha Sonawane[5]

Student, Computer Department, SSJCOE, Dombivli, India[1, 2, 3, 4]

Professor, Computer Department, SSJCOE, Dombivli, India[5]

Abstract: The wired network to wireless network is a worldwide trend in the past few days. The suspicious or malicious activities are detected using intrusion detection system. The most important and unique application is Mobile Ad hoc NETwork (MANET). In this paper, we have implemented a new intrusion-detection system called Enhanced Adaptive Acknowledgment (EAACK) particularly modelled for MANETs. In this paper, we are focus on Denial of Services Attack.

Keywords: Enhanced Adaptive Network, Dos Attack, MANETs, Digital Signature Algorithm.

I. INTRODUCTION

In past few days due to their natural mobility and scalability wireless network always preferred to improved technology and reduced costs. Intrusion detection is defined as a process of monitoring events occurring in network and it analysis them for possible intrusion. The responsibility of intrusion detection system is to detect malicious behaviour. Manet is a collection of mobile nodes which are equipped with wireless transmitter and receiver. Both wireless transmitter and receiver are connected with each other via bidirectional wireless link. Manet consists of two types of networks, one is single-hop and another is multi-hop. In a single-hop network, all nodes within the same range communicate directly with each other while in a multi-hop network, nodes rely on other intermediate nodes to transmit out of their radio range. Data collection, feature collection, analysis, action are the functions of intrusion detection system.

The aim of this project is to improve security of the system and identify problems or attacks which are based on the security policies.

II. BACKGROUND

A. IDS IN MANETS

MANETs is the wireless network of the mobile device. In the network function, nodes represent as server, router, client. Intrusion detection system is classified into two types as Network based IDS (NIDS) and Host based IDS (HIDS)[4]. There are also two more techniques namely, signature based IDS and anomaly based IDS. Due to the limitation of most MANET routing protocols,[3] nodes in MANETs consider that other nodes always cooperate with each other to trusted data. Due to this assumption the attackers will leave an chance to achieve an significant effect on the network with just one or two compromised nodes. If MANET can be detect the attackers as they enter the network, we will be able to delete the damages created by those sucessive nodes .We have introduced three existing approaches, namely Watchdog, Adaptive ,and Acknowledgement(AACK), TWOACK.

1) Watchdog:

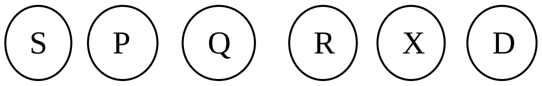
This scheme was introduced by Martietal. The goal of this scheme is to enhance the throughput of network with the presence of malicious nodes. Watchdog scheme have two parts, they are Watchdog and Pathrater. The responsibility of watchdog is to detect malicious misbehaviour by listening to its next hop's transmission. At certain period of time if Watchdog node overhears, that means its next node is unsuccessful to transfer the packet. It expands its failure counter. In this condition, the Pathrater will unite with the routing protocols so that it avoids the reported nodes in future transmission. The researches and implementations have proved that the Watchdog scheme is one of the efficient and popular schemes. This scheme fails to detect malicious misbehaviours with the presence of the following conditions:

1) Ambiguous collisions
2) Collisions near receiver
3) Transmission power is limited
4) Generate the false misbehaviour report
5) Collusion
6) Partial dropping

2) Twoack:

As we know that in Watchdog schemes, there are six weaknesses, those researchers' proposed new approaches to solve these issues. TWOACK was proposed by Liuetal is most important approaches between them. TWOACK is not a Watchdog-based scheme but is used to determine the receiver collision and the problem of limited transmission power of Watchdog.

Fig 1 shows the working process of TWOACK. First Node P forwards Packet 1 to node Q, then, node Q forwards Packet 1 to node R. When Packet 1 is received by node R as it is two hops away from node P, it generates a TWOACK packet, this contains reverse path from node P to node R, and sends it back to node P.



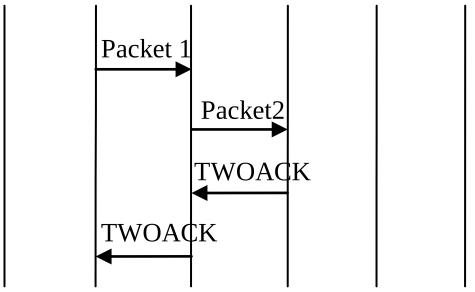


Fig1: TWOACK Scheme

3) Aack:

This stands for Adaptive Acknowledgement. AACK is based upon the scheme TWOACK, Sheltamietal proposed a new scheme called AACK. AACK is an acknowledgment-[2] based network layer like TWOACK. It is measured as a combination of a scheme called TWOACK and acknowledgment scheme that is Acknowledge (ACK). TWOACK notably reduced network overhead while still capable of preserve the same network as differentiated to AACK. .

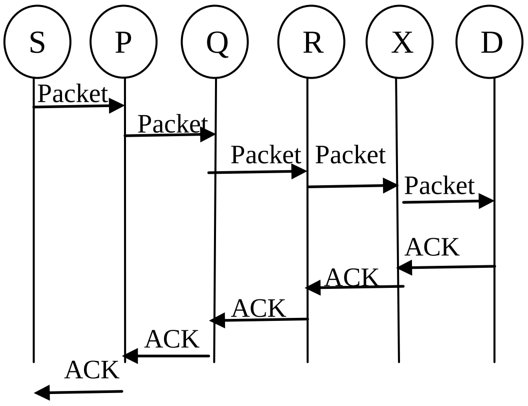


Fig2: AACK Scheme

The Fig. 2, the source node S send Packet 1 without any overhead except P of flag indicating the packet type. All the intermediate nodes proceed this packet.[2] When the destination node D receives Packet, it is essential to send reverse ACK acknowledgment packet to the source node S along the same path. If the source node S receives acknowledgment packet within a assumed time period, then the packet transferred from node S to node D is successful. If no then, the source node S will change to TACK scheme that will send a TACK packet.

B. Digital Signature:

Digital signature is a important section of cryptography. Where cryptography deals with the study of mathematical techniques that are related to characteristics of information security that is confidentiality, integrated data and evidence. Digital signature is a widely used approach to ensure the confirmation, integrity, [2] and non denial of MANETs.

Digital signature schemes are being divided into the following two categories.

1) Digital signature with supplementary information: In this original message is essential in the signature verification algorithm. Examples it include DSA.

2) Digital signature with message recovery: In this type of scheme it does not occupy any other information besides the signature itself will do verification of process. Examples it include RSA.

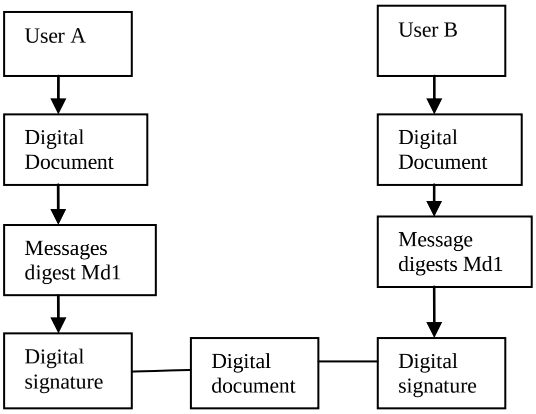


Fig3: Digital Signature

C. ACK:

The ACK is basically an end-to-end acknowledgment scheme. It is a unit of the hybrid scheme in EAACK .That its goal is to reduce network elevated when there is no network misbehaviour. In ACK mode, node S first sends out an ACK data packet to the destination node D.[5] If all the intermediate nodes along the path of nodes S to D are mutual so node D successfully receives packet, node D is essential to send back an ACK acknowledgment packet along the same path but in a reversed order.[4] Within a predefined time period, if node S receives , then the packet transmission from node S to node D is successful. Otherwise, node S will shift to S-ACK mode by sending out an S-ACK data packet to find the misbehaving nodes in the path.

D. S-ACK:

The S-ACK scheme is an new model of the TWOACK scheme was introduced by Liuetal. The principle is to let every three repeated nodes work together to detect misbehaving nodes. For every three successive nodes in the path, the 3rdnode has a necessary task to send an S-ACK acknowledgment packet to the 1stnode.[3] The purpose of launching S-ACK mode is to recognize misbehaving nodes in the presence of collision created at receiver or transmission power is limited.

E.MRA:

The MRA scheme is designed to analyse the weakness of Watchdog schemes. When it fails to notice misbehaving nodes with the presence of generate false misbehaviour report. The false misbehaviour report can be generated by malicious attacker to incorrectly report true nodes as malicious. This attacks the entire network when the attackers break down enough nodes which results in a network division.[4] The centre of MRA scheme is to authenticate whether the destination node has received the

DOI 10.17148/IJARCCE.2016.52134

report of missing packet through a different path.[4] To initiate the MRA node, the source node first find out on its limited knowledge bases and then seeks for another alternative path towards its destination node. If there is no another existing path, then the source node will starts with a DSR path and then request to find another path . Due to the nature of MANETs, it is common to find out multiple paths between two nodes.

III.SIMULATED RESULTS

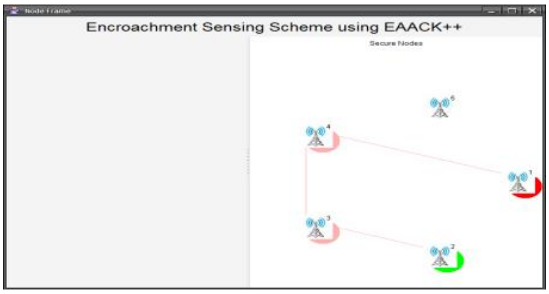


Fig.4 Server

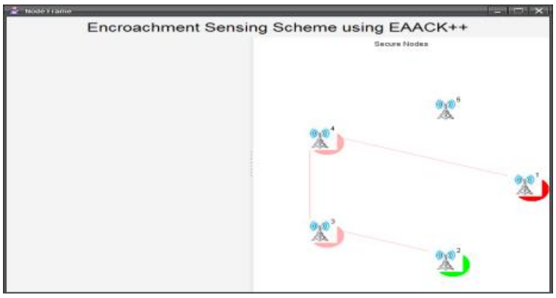
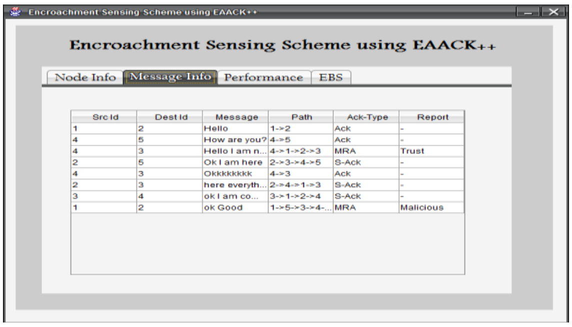
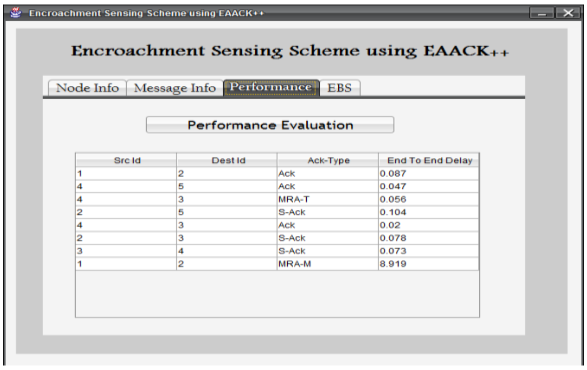


Fig.5 Node information


Encroachment Sensing Scheme using EAACK++
Encroachment Sensing Scheme using EAACK++
Node Info
Message Info
Performance
EBS

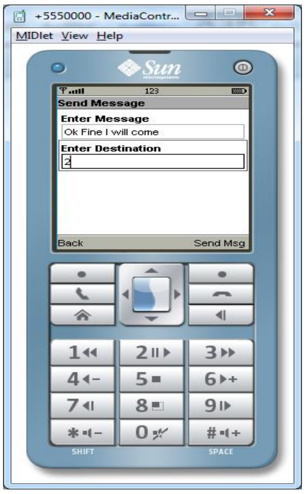
Src Id	Dest Id	Message	Path	Ack-Type	Report
1	2	Hello	1->2	Ack	-
4	5	How are you?	4->5	Ack	-
4	3	Hello I am n...	4->1->2->3	MRA	Trust
2	5	Ok I am here	2->3->4->5	S-Ack	-
4	3	Okkkkkkkk	4->3	Ack	-
2	3	here everyth...	2->4->1->3	S-Ack	-
3	4	ok I am co...	3->1->2->4	S-Ack	-
1	2	ok Good	1->5->3->4-...	MRA	Malicious

Fig.6 Message Transferd


Encroachment Sensing Scheme using EAACK++
Encroachment Sensing Scheme using EAACK++
Node Info
Message Info
Performance
EBS
Performance Evaluation

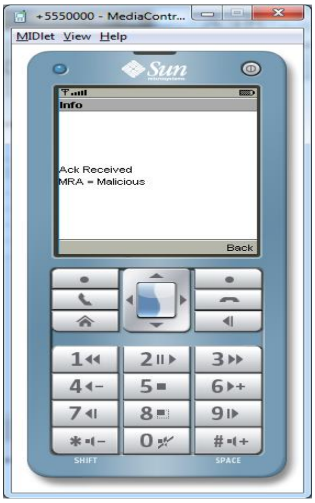
Src Id	Dest Id	Ack-Type	End To End Delay
1	2	Ack	0.087
4	5	Ack	0.047
4	3	MRA-T	0.056
2	5	S-Ack	0.104
4	3	Ack	0.02
2	3	S-Ack	0.078
3	4	S-Ack	0.073
1	2	MRA-M	8.919

Fig.7 Performance info



Send Message
Enter Message
Ok Fine I will come
Enter Destination
2

Fig.8 Client side message



Info

Ack Received
MRA = Malicious

Fig.9 Server side message

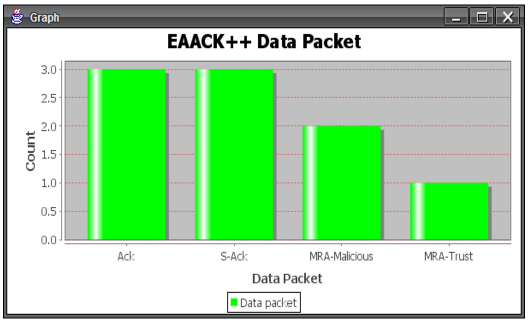


Fig.10 Graphical analysis

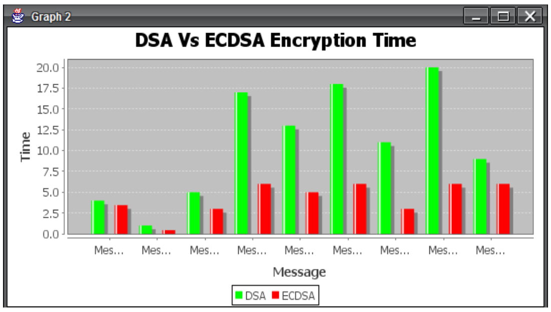


Fig.11 Encryption of message

DOI 10.17148/IJARCCE.2016.52134

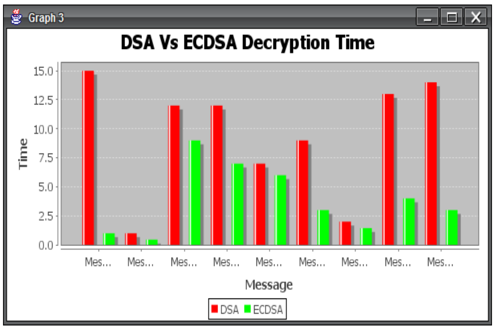


Fig.12 Decryption of message

IV. CONCLUSION

Before determining a network traffic is a potential threat to a network, there is a need for IDS to have a method into find out whether it is malicious or not. This search has brought a new method to identify a fast time based detection of attack or intrusion. This method is used to identify inconsistency this inconsistency is based on the number of connection made in 1 second. For further validation, the methodology will be implemented on a different set of real network traffic. In this research paper, we have proposed a new ID named EAACK protocol specially modelled for MANETs and compared it against other popular mechanisms through simulations. The results signify for positive performances against Watchdog, TWOACK, and AACK in the situations of receiver collision, limited transmission of power, and generated false misbehaviour report.

To increase the advantages of our research work, we have planned to investigate the following points in our future research:

1) To reduce the network created overhead caused by digital signature the hybrid cryptography is adopted.
2) To examine the possibilities of adopting a key exchange techniques to delete the requirement of keys which are pre-distributed.
3) The performance of EAACK in networking environment is tested instead of software simulation.

ACKNOWLEDGMENT

It is our great sense of satisfaction that we represent our real undertaking on practical computing in the form of project work. We wish to express our gratitude to **Dr. J.W. Bakal** (Principal) & **Prof. Rodge** (HOD of Computer Department) for providing us opportunity to undertake this project. We would like to thanks **Prof. Uttara Gogate** for providing us her valuable advice. We are thankful to Prof. Manisha Sonawane giving time to time tips & helping in every work of project. We express our gratitude for all the teachers for their technical & moral support for selection our project. We also thank all our friends for helping us when we needed most.

REFERENCES

[1] R. H. Akbani, and S. Patel, also D. C. Jinwala, “in MANET the dos attack : A survey,” India.

[2] N. Kang, E. Shakshuki, and T. Sheltami, which inform us regarding “Detecting malicious misbehavring of nodes in MANETs., was held in Paris, France.

[3] N. Kang, and E. Shakshuki, also T. Sheltami has the information of “Acknowledgement of MANETs is detected,”

[4] Cuppen, F.& Miege, A. Alert Correlation in a supportive Intrusion Detection Framewok. In happening of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]

[5] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005) .Network Traffic are categorized Using energetic State Classifier. In Proceeding of IEEE Conference.