International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

A New Secure Intrusion-Detection System for MANETs

Radhika Amareshwari, Assistant Professor,
P. Haritha, Assistant Professor,
S.Ramanjaneyulu, Assistant Professor,
Geethanjali College Of Engineering And Technology,Cheeryal, R.R.Dist.

ABSTRACT : The migration to wireless network from wired network has been a global trend in the past few decades.A new technique EAACK (Enhanced Adaptive Acknowledgement)method designed for MANET was proposedfor intrusion detection. Due to some special function of Manets only prevention is not good for managing thesecure networks. In this case detectionshould be focused as another part beforean attacker can damage thestructure of system. Compared to up todate approaches, our approach demonstrates higher malicious-behavior detection rates in sure circumstanceswhereas doesn't greatly have an effect on the network.

Keywords ***-****Digital signature,Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile AdhocNETwork (MANET).*

I. INTRODUCTION

MANET (Mobile Ad hoc network) is an IEEE 802.11 framework which is a collection of mobile nodes equipped with both a wireless transmitter and receiver communicating via each other using bidirectional wireless links. Fig 1 showsthis type of peer to peer system infers that each node or user in the network can act as a data endpoint or intermediate repeater. Thus, all users work together to improve the reliability of network communications. MANETs are self -forming, self-maintained and self-healing allowing for extreme network flexibility, which is often used in critical mission applications like military conflict or emergency recovery.But this communication range is limited to transmitter range. That means two nodes cannot communicate with each other if the nodes are beyond the communication range. Manet solves this problem by allowing intermediate nodes for data transmission this achieved by dividing network in two types as single hope and multihop network. In single hope network the nodes can directly communicate with each other within the communication range. But in multihopnetwork nodes are rely on intermediate nodes if the end node is not within the range of communication range [1].

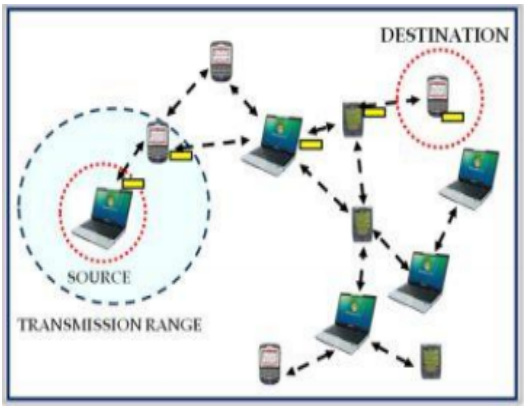

Fig 1 MANET Architecture

In general, MANETs are vulnerable based on the basic characteristics such as open medium, changing topology, absence of infrastructure, restricted power supply, and scalability. In such case, Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS) [2] [3].

Owing to these distinctive characteristics, MANET is becoming additional and additional wide enforced within the trade. However, considering the very fact that MANET is in style among crucial mission applications, network security is of important importance. Sadly, the open medium and remote distribution of MANET create it prone to varied varieties of attacks.

For instance, as a result of the nodes lack of physical protection, malicious attackers will simply capture and compromise nodes to attain attacks. specially, considering the very fact that the majority routing protocols in MANETs assume that each node within the network behaves hand and glove with different nodes and presumptively not malicious [5], attackers will simply compromise MANETs by inserting malicious or no cooperative nodes into the network. What is more, as a result of MANET's distributed design and dynamical topology, a conventional centralized observance techniqueisn't any longer possible in MANETs.

II. RELATED WORKS

N. Kang, E. Shakshuki and T. Sheltami proposed a scheme called Enhanced Adaptive Acknowledgement (EAACK). This scheme aims to overcome four of the weaknesses in traditional Watchdog mechanism, namely, ambiguous collisions, receiver collisions, limited transmission power and false misbehavior. But there is no authentication for acknowledgements. The functions of detection scheme largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. So this scheme is not much efficient.

Elhadi M. Shakshuki proposed EAACK which was designed with the implementation of RSA and DSA digital signatures using DSR routing protocol. Performance evaluation was done and results were obtained. But this EAACK has no provision for handling link breakage and malicious source node scenario. Later the introduction of digital signature to prevent the attacker from forging acknowledgment packets was proposed. It used a new protocol for better security using hybrid cryptographic technique to reduce the overhead caused by digital signature.

MANETs into industrial application. So it is vital to address its security issues. Such existing IDSs in MANETs are 1) Watchdog 2) TWOACK and 3) AACK.

Watchdog: Watchdog improves the throughput of the network even in the presence of attackers. It has two parts namely Watchdog and Path rater. It detects malicious nodes by overhearing next hop's transmission. A failure counter is initiated if the next node fails to forward the data packet. When the counter value exceeds a predefined threshold, the node is marked malicious. The major drawbacks are 1) ambiguous collisions 2) receiver collisions 3) limited transmission power 4) false misbehavior report 5) partial dropping 6) collusion.

TWOACK:TWOACK overcomes the receiver collision and limited transmitted power limitation of Watchdog. Here acknowledgment of every data packet over every three consecutive nodes is sent from source to destination. If ACK is not received in a predefined time, the other two nodes are marked malicious. The major drawbacks are 1) Increased overhead 2) Limited battery power 3) Degrades the life span of entire network fig 2 shows.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

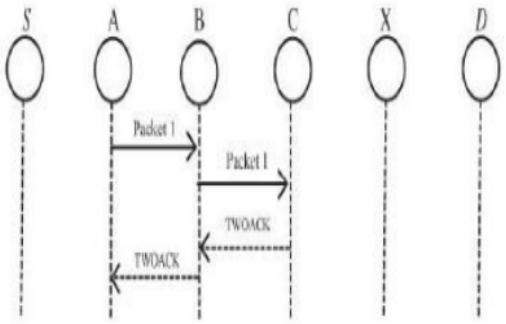

Fig: 2 Two ACK IDS for MANETs

AACK: Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks is that it suffers from 1) False misbehavior report2) Forged acknowledgment packets.

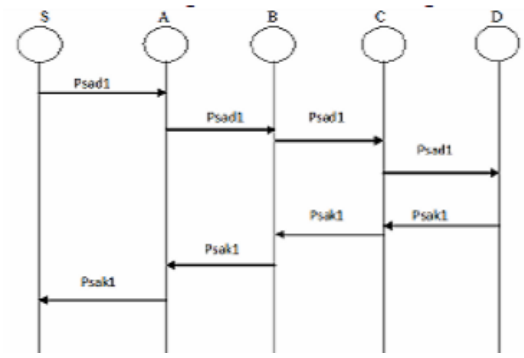

Fig: 3 END-END ACK for MANETs

III. PROBLEM DEFINITION

(EAACK) i.e. Enhanced Adaptive Acknowledgement is design to solve the three of six weaknesses of watchdog scheme namely

1) Receiver collision

2) Limited transmission power

3) False misbehavior.

A. Receiver Collisions: 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.

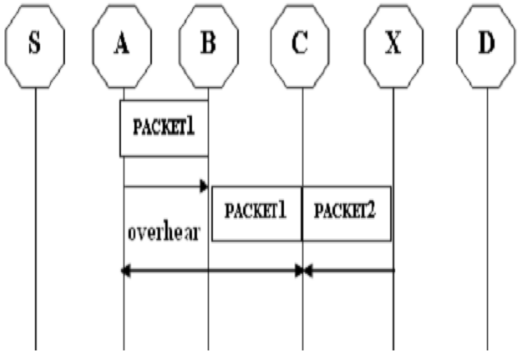

Figure 4: Receiver Collision

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.

B. Limited transmission power:- As shown in the figure.5 of limited transmission power to manage battery resources node B limits its transmission power so that it is very strong to overheard by node A after transmitting power but it's too weak to reach at node C because transmission power is reduced at certain limit.

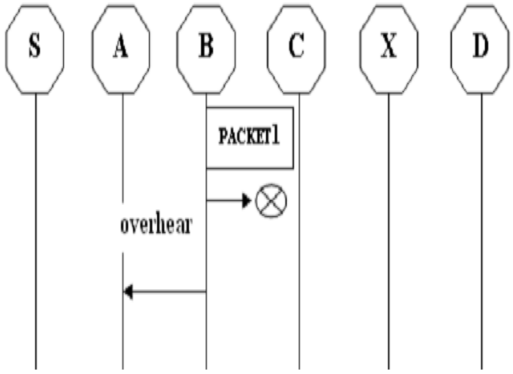

Fig.5 Limited Transmission Powers

C. False misbehave :- As shown in the fig.6 even though node A and node B send packet1 successfully to node C node A still inform node B as misbehaving due to open medium and remote distribution of typical manets.

Attackers can add one or two nodes to achieve this false misbehavior report attack.

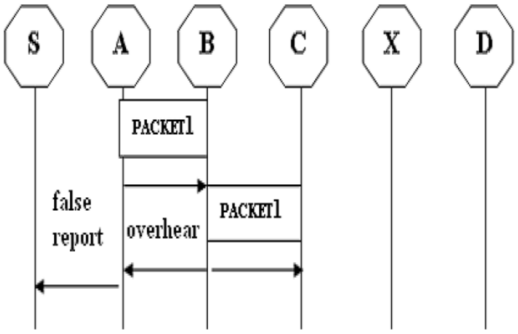

Fig.6 False Misbehave

Two ack and AACK can solve this problem of limitedpower transmission as well as receiver collision but both are fail to solve the problem of false misbehavior attack. In order to solve receiver collision, limited transmission power as well as false misbehavior attack the EAACK (enhanced adaptive acknowledgement) is introduced [1].

IV. SCHEMEDESCRIPTION

EAACK is consisted of 3 major components, namely, ACK, secure ACK (S-ACK), and misconduct report authentication (MRA).

A.ACK: ACK is basically an end-to-end acknowledgement scheme. It acts as a part of the hybrid scheme in RRACK, aiming to reduce network overhead when no network misbehavior is detected. If ACK scheme fails the node 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. 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.

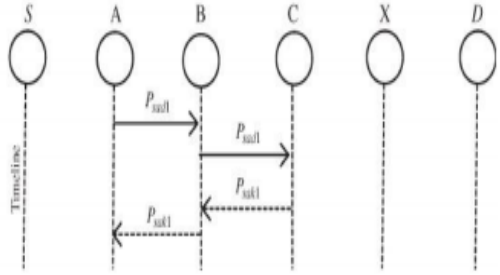

Figure 7: Secure Acknowledgement

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. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.By adopting an alternative route to the destination node, 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.

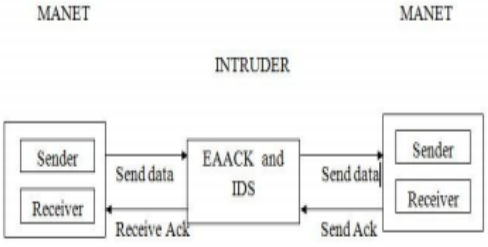

Figure 8: System Architecture

Parameters	Existing system	Proposed system
Overhead bits	More	Less

Security	Less	More
Limited transmission power problem	Not solved	Solved
Malicious nodes	Not detected	Detected
Receiver collision	occurs	Not occurs
False misbehave problem	Not solved	Solved
Attacks	Possible	Not possible

D. Digital Signature: EAACK is an acknowledgment-based ID'S. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

V. CONCLUSION

In this research paper, we have study a novel INTRUSION-DETECTION SYSTEM named EAACK protocol specially designed for MOBILE AD-HOC NETWORKs and compared it against other popular mechanisms in different scenarios through simulations.So many drawbacks of existing systems are overcome in this system that is used for discovering malicious nodes and attacks on Manets. The EAACK system is very much secured than the existing system. The proposed system is solving the three of six weaknesses found in existing system.

REFERENCES

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

[2] Investigating Intrusion and Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes Marjan Kuchaki Rafsan,Ali Movaghar and Faroukh Koroupi,World Academic of Science Engineering and Technology 44 2008.

[3]L.Zhou,Z.J.Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, [4] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad,2009."Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network". CRC PRESS Publishers.

[4]Kalman Graffi and Ralf Steinmetz, "Detection of Colluding Misbehaving Nodes in Mobile Adhoc and Wireless Mesh Networks," In: IEEE Global Communications Conference (IEEE GLOBECOM), Nov 2007.

[5] Kejun Liu and VarshneyMay, "An acknowledgment-based approach for the Detection of routing misbehavior in MANETs," IEEE Trans.Mobile Comput., vol. 6, no. 5, May 2007.

[6] Nodal Nasser and Chen Y, "Enhanced Intrusion Detection Systems for discovering malicious nodes in mobile Adhoc network," in Proc.IEEE Int.Conf. Commun. Glasgow, Scotland, Jun 2007.

[7] Rajaram and Gopinath, "Efficient Misbehavior Detection System for MANET," Dec 2010

[8]Rajyalakshmi and Anusha, "Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System, "July 2013.

[9] Rivest and Adleman, "A method for obtaining digital signatures and public-key

cryptosystems," Commun.ACM, vol. 21, no.2, pp. 120–126, Feb 1983.

[10]"Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol"Ahmed M. Abdulla, Imane A. Saroitb, Amira Kotbb, Ali H. Afsaric a* 2010 Published by Elsevier Ltd.