ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization *Vol.3, Special Issue 5, May 2015*

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)
on 5th & 6th May 2015, Organized by
Department of CSE, Vemana Institute of Technology, Bengaluru, India

A Survey on IDS and A Mechanism for Detecting Malicious Nodes Using Enhanced Secure Acknowledgment (ES-ACK)

KiranAradhya S T [1], Nagesha A G [2], ManojAithal S [3], Hemanth Kumar N P [4],

[1]PG Scholar, Department of CSE, Acharya Institute of Technology, Bangalore, Karnataka, India

[2]Associate Professor, Department of CSE, Acharya Institute of Technology, Bangalore, Karnataka, India

[3]PG Scholar, Department of CSE, Alva's Institute of Engineering and Technology, Mangalore, Karnataka, India

[4] Assistant Professor, Department of CSE, Alva's Institute of Engineering and Technology, Mangalore, Karnataka, India

ABSTRACT: Wireless communication represents a major industrial stake in the coming years. The ability to be moved from one place to another and to make larger brought by wireless network made it possible in many applications. It targets applications in harsh environments such as war zones, emergency recovery, power plants and warships etc. MANETs is one among the wireless technology which is widely used. MANETs does not need any pre-configurations or permanent network architecture or infrastructure compared to wired technology. The wireless links between the nodes together with the active or changing nature of ad hoc network, increases the challenges of design and implement intrusion detection during the attacks. The intrusion detection system is achieved through a mechanism called Enhanced Secure Acknowledgment (ES-ACK) which is more elegant than watchdog. Another challenging issue in MANETs is the data integrity, which is achieved through Message Authentication Code (MAC).

KEYWORDS: Mobile Ad hoc NETwork (MANET), Watchdog, Enhanced Secure Acknowledgment (ES-ACK),Digital Signature, Intrusion Detection System(IDS).

I. INTRODUCTION

Mobile Ad hoc NETwork (MANET) is an aggregate of mobile nodes to provide necessary materials with both wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Accessing the remote access industries and control using wireless networks are becoming more and more popular. The advantage of wireless networks is the ability to allow data communicating each other between different organizations and maintain to reach the remote access. This communication is limited to the range of Transmitters. Two nodes cannot communicate with each other when if their distances between the two nodes the range of their two nodes is beyond the communication range of their own.

MANET solves the difficulty of the above problem by allowing intermediate organizations to give the data to group and transmits it. MANETs are of two types of networks namely, single-hop and multihop. In a single-hop network, nodes within the same radio range and will communicate directly with each other. In a multihop network, nodes rely on intermediate nodes to transmit the data if the destination node is out of their radio range using the intermediate nodes they will communicate each other.

MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; hence, nodes move randomly without any fixed infrastructure. MANET is capable of creating a self-arranging and self-continue without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal arranging and quick setup make MANET ready to be used in emergency

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

situations where an infrastructure is not available or not feasible to install in scenarios like natural calamities or human-induced effects, military property, and medical emergency circumstances.

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs.

II. SURVEY ON MANETS

A. Which wireless technology for industrial wireless sensor networks?

Wireless mesh networking has emerged in the recent years as a promising design paradigm for next-generation wireless communication networks with interesting characteristics such as self-organizing and auto-configurable topology, and *ad hoc* routing concept. These properties promise substantial benefits in terms of operating and maintenance costs of the communication infrastructure in industrial installations. They also ease the development of "killer applications" such as condition monitoring or condition-based maintenance (CBM) that requires flexible and cost-effective sensor networks. Wireless technologies help engineers achieve these objectives. However, most of the existing general-public wireless-communication technologies do not take into account the industrial requirements. There exists proprietary radio-communication technologies for industrial use (e.g., Wavenis), but the benefits of interoperability (and thus, cost) are lost from multivendor solutions. Developing and promoting industrial wireless-communication standards help industrial end users preserve the expected benefits of wireless technologies. We propose to review the state of the art of current industrial wireless networking standards.

B. Denial of service attacks in wireless ad hoc networks

Due to the absence of a central trusted router in WANETs, nodes have to trust each other when routing data packets. The required mutual trust makes WANETs vulnerable to misbehaviors that may arise for several reasons:

1. Faulty nodes may misbehave due to configuration errors or some hardware errors.

2. Selfish nodes may not cooperate in network protocols in order to save energy.

3. Malicious nodes mount attacks with the intent of damaging the network or extracting valuable information from the network. Regardless of misbehavior type, it may cause a performance degradation of the whole network. Therefore, there is a need to secure network protocols in WANETs.

C. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks

Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth an d the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g ., wired an d stationary) network. Expensive and cumbersome security mechanisms can delay or prevent such exchanges of routing information, leading to reduced routing effectiveness, and may consume excessive network or node resources, leading to many new opportunities for possible Denial-of-Service attacks through the routing protocol.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

D. A survey on intrusion detection in mobile adhoc networks

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defense, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defense to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system.

Some assumptions are made in order for intrusion detection systems to work. The first assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviours, as intrusion detection must capture and analyze system activity to determine if the system is under attack.

E. ad hoc mobile wireless networks routing protocols – a review

In general, on-demand reactive protocols are more efficient than proactive ones. On-demand protocols minimize control overhead and power consumption since routes are only established when required. By contrast, proactive protocols require periodic route updates to keep information current and consistent; in addition, maintain multiple routes that might never be needed, adding unnecessary routing overheads. Proactive routing protocols provide better quality of service than on-demand protocols. As routing information is constantly updated in the proactive protocols, routes to every destination are always available and up-to-date, and hence end- to- end delay can be minimized. For on-demand protocols, the source node has to wait for the route to be discovered before communication can happen. This latency in route discovery might be intolerable for real-time communications.

III. BACKGROUND STUDY

Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Path rather. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listening to its next hop's transmission. If a 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 Path rater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field.

A. Disadvantages of Watchdog:

1. Ambiguous collisions.
2. Receiver collisions.
3. Limited transmission power.
4. False misbehavior report.
5. Collusion.
6. Partial dropping.

IV. PROPOSED SYSTEM

The security in MANETs is defined as a combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, and non-repudiation. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

A. Problem Statement

Watchdog which was the prominent IDS for MANETs until the minor flaws such as Ambiguous collisions, Receiver collisions etc. were detected. To overcome these flaws new mechanism is proposed

B. Objective

To develop an intrusion-detection mechanisms to protect MANET from attacks.

C. *Methodology*

S-ACK 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 packet transmitted over consecutive nodes along the path from the source to the destination.

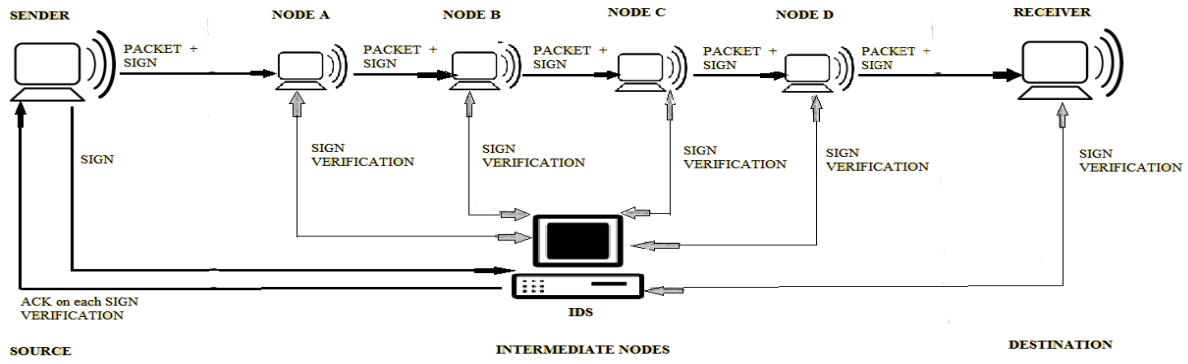

Fig 4.1 S-ACK scheme Architecture

V. SYSTEM DESIGN

UML has been developed as a language for modelling object- oriented systems. Its use has however widely been spread out. Today UML is used for system specifications. In different domains UML is used for specification and standardization of different systems or parts of the systems. UML is becoming a standard tool for software and system engineers.

A. Dataflow diagram

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system, which can later be elaborated.

The sender would select the file for the transmission and creates a Message Authentication Code (MAC) for data integrity with its appropriate key to the transmission file. Then File is ciphered for the purpose of security using DES algorithm by the user defined key. Then a signature is generated, which is sent to IDS (intrusion detection system) which plays a major role in monitoring of nodes from source to destination. The encrypted file along with signature is transmitted to neighbouring node (in this case let us consider Node A).In each intermediate nodes, signature verification is done with respect to IDS (intrusion detection system).If the verification yields success then it is transmitted to next neighbouring node else it would alert the sender of an intrusion or the misbehaviour of the nodes. Receiver gets the key from the file which is used to generate the MAC. And receiver creates the MAC and compared it

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

to the MAC which is received from the file. If there is no change in the tow MAC means then the file is not changed and the integrity is proved.

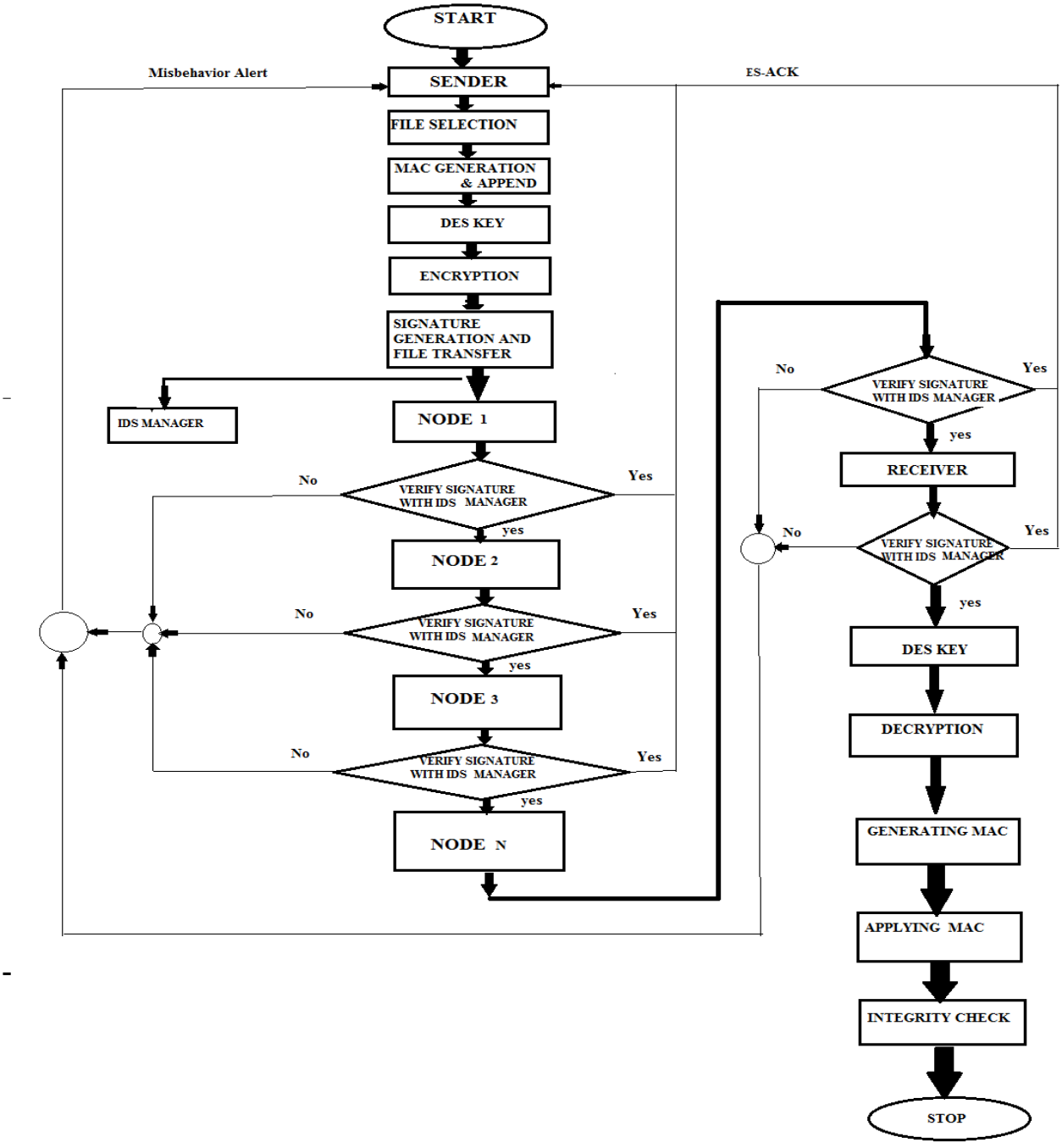

Fig 5.1 Dataflow Diagram

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization *Vol.3, Special Issue 5, May 2015*

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

VI. RESULTS

Sl.no	IDS	WORKING MECHANISM	RESULTS
1	WATCHDOG	Consist of two parts namely Pathrater and watchdog. The Watchdog detects misbehaviour by promiscuously listening to the next node. And if it overhears that the next node fails to forward the packet it increases its failure counter .when these failure count exceeds the threshold then it reports it as misbehaving.	Watchdog scheme fails to detect malicious misbehaviour in the presence of ambiguous collision, receiver collision, limited transmission power, collusion... etc.
2	TWOACK [2]	TWOACK scheme where each node is requested to send back an acknowledgment packet to the node that is two hops away from it.	The acknowledgment 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	Adaptive ACKnowledgment (AACK) [2]	Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK).	TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.
4	Enhanced Secure Acknowledgement (ES-ACK)	In case of this proposed system, the whole burden of Acknowledgement is taken by IDS manager as shown in the fig 4.1. The intermediate nodes can only concentrate on transmission of the data to the next node.	It resolves most of the watchdog's weaknesses, and can actively detect malicious nodes even in the presences of false misbehaviourreport, this is achieved through Digital Signature.

VII. CONCLUSION

The MANETs are used in critical missions hence detection of misbehaviour nodes is required immediately. The proposed system deals with the IDSfor MANETs and in proposed system it overcomes the most of the weakness of watchdog. And also integrity is one of the major aspects of MANETs, which is achieved through MAC in the proposed System.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015

International Conference On Advances in Computer & Communication Engineering (ACCE - 2015)

on 5th & 6th May 2015, Organized by

Department of CSE, Vemana Institute of Technology, Bengaluru, India

In future following works can be conducted:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature;

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre-distributed keys.

REFERENCES

[1]. Which Wireless Technology forIndustrial Wireless Sensor Networks? The Development of OCARI Technology Khaldoun Al Agha, Senior Member, IEEE, Marc-Henry Bertin, Tuan Dang,
[2]. EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE.
[3]. A Survey on Intrusion Detection in Mobile Ad Hoc Networks Using Enhanced Adaptive Acknowledgment.
[4]. Wireless/Mobile Network Security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 170 – 196 °c 2006 Springer Chapter 7 A Survey on Intrusion Detection in Mobile Ad Hoc Networks.
[5]. Distributed and Cooperative Hierarchical Intrusion Detection on MANETs.
[6]. A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANETs.
[7]. A Study On Enhanced Adaptive Acknowledge (EAACK) Scheme In Receiver Collisions – An IDS In Wireless Mobile Ad-Hoc Networks.
[8]. International Journal of P2P Network Trends and Technology (IJPTT) – Volume 8 – May 2014 ISSN: 2249-2615 http://www.ijpttjournal.org Page 5Enhanced Secure Intrusion Detection System in MANETs.