Acknowledgement Based Intrusion Detection System in Mobile Ad-Hoc Networks using EAACK

Ms. Pallavi N. Ratnaparkhi
Department of CS/IT
G.H. Raisoni Institute of Engineering &
Technology for Women, Nagpur, India

Mr. Ravindra D. Kale
(Asst. Professor)
Department of CS/IT
G.H. Raisoni Institute of Engineering &
Technology for Women, Nagpur, India

***Abstract*— From few decades, Mobile Ad hoc NETworks (MANETs) are becoming a very popular research topic, because of no fixed infra-structure for MANETs. It's an attractive technology for many applications like in military use. The mobility and scalability brought by MANETs in wireless network made it possible in many applications, the fact that MANET is popular among critical mission applications like military use or emergency recovery, network security is of vital importance. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In the proposed work, a new ACKnowledgement based intrusion-detection system will be designed for MANETs using hybrid cryptography techniques. It will demonstrate higher malicious-behavior-detection rates in certain circumstances while it does not greatly affect the network performances. The proposed work will be on reducing the power consumption, the network delays and improving the efficiency of MANETs while detecting misbehaving reports and will reduce network overhead.**

Keywords— **Mobile Ad-hoc Network (MANET), Intrusion Detection System (IDS), Enhanced Adaptive Acknowledgement (EAACK), AACK, TWOACK**

I. INTRODUCTION

A Mobile Ad-hoc NETwork (MANET) is an infrastructure-less network consisting of self- configuring mobile nodes connected by wireless links [10]. Nodes rely on each other to store and forward packets. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery, network security is of vital importance [1]. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. Furthermore, MANETs are highly vulnerable for passive and active attacks because of their open medium, rapidly changing topology, lack of centralized monitoring. Encryption and authentication solutions, which are considered as the first line of defense, are not sufficient to protect MANETs from packet dropping attacks [3].

In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. An intrusion detection system (IDS) is a device or software application that monitors network activities for malicious activities or policy violations and produces reports to a management station. An intrusion detection system (IDS) is a device or software application that monitors network activities for malicious activities or policy violations and produces reports to a management station. A new intrusion detection system named Enhanced Adaptive Acknowledgement (EAACK) specially designed for detecting malicious nodes in MANETs, which provides more secure, valid and authentic data transmission [1]. This technique for intrusion-detection will be used to enhance the proposed system performance merits by reducing the power consumption, reduced network delays and improved efficiency in MANETs with secure and authentic data transmission using more efficient hybrid cryptography techniques.

This paper gives us the overview of the new intrusion detection system which is acknowledgement based. In the first section it gives the introduction of the MANET and the IDS, in second section it gives somewhat objectives of the system, the third section gives the idea of related work which has been done in the past years, fourth section gives us architecture of proposed system, fifth section gives the flow or basic concept of this IDS, the sixth section gives us idea of expected outcome and the last section seventh gives us the summary of the paper.

II. OBJECTIVES OF PROPOSED WORK

The main objectives of the intrusion detection system are as follows

- **Detecting attacks**: Such a system detects security threats and attacks and when they happen, by providing real-time network monitoring. We will devlope such a system that will easily can detect the intruders present in the network and would not affect the rest of the network communication.

- **Offer information**: If this system detects an attack, then it will put forward information about the attack i.e. which type of attack has been occurred in search for the remedies for such attacks.

- **Take corrective steps**: Once an attack is detected by the system, the active systems also take measure to tackle the attack and take some corrective or preventive steps..

- **Storage**: It also stores the events either locally or otherwise in case of an attack.

- **A good system model**: It is designed for MANETs which will detect intruders.

III. RELATED WORK

Many noteworthy contributions are done in area of the wireless networks for intrusion detection by many researchers. Some of them can be discussed here.

1. Watchdog is used for improving the throughput of network in the presence of malicious nodes. It detects the misbehavior by listening to the next hop's node [2]. But it has some weaknesses which are improved in next technologies.
2. The TWOACK is the next IDS which somewhat reduced the shortcomings in watchdog. It acknowledges every data packet over network between three consecutive links and detects misbehaving links. It is used to reduce the two limitations of Watchdog technique i.e. receiver collision and limited power transmission [2].
3. AACK is Acknowledgment based scheme it may be consider as combination system of an Enhanced TWOACK (E-TWOACK) scheme [5] and End-to- End Acknowledgment scheme. They also described the AODV protocol and the black hole attacks.

IV. THE PROPOSED SYSTEM ARCHITECTURE

The proposed system will adopt a new hybrid cryptography technique and will help to further reduce the network overhead and delay. Also it will adopt more effective key exchange mechanism to eliminate the requirement of pre-distributed keys and reducing the parameters. The architecture of this system can be shown in the figure given below.

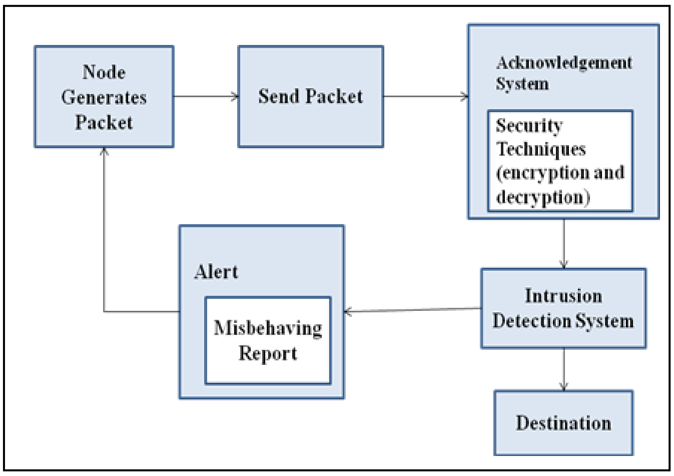

Fig.(1) The Proposed System Architecture

In the above fig.(1), the acknowledgement system present here is used for acknowledging the transmission control flow and uses various security techniques for encryption and decryption of data. The intrusion detection system is used for detecting the malicious nodes present during communication in the network and if any malicious or misbehaving node is found it will send the misbehaving report to the source node otherwise it will directly send the encrypted packet to the destination node.

V. RESEARCH METHODOLOGY TO BE EMPLOYED

A new intrusion detection system flow diagram is designed to detect the malicious nodes present in the network. It is shown in the following diagram figure (2). It is 8 step acknowledgement plus detection mechanism.

The following steps demonstrates the actual control flow of system during data packet transmission

1. Source node sends request to destination if it is available or not.
2. Destination node sends ACK to source node of it is available.
3. Source requests to destination for its signature for checking is it malicious node or not
4. Destination send its signature to base station
5. Base station verifies the signature
6. Source receives a challenge packet ACK from Destination for signature verification
7. Encrypted data is sent from source to destination.
8. ACK of receipt of data is sent from destination to source.

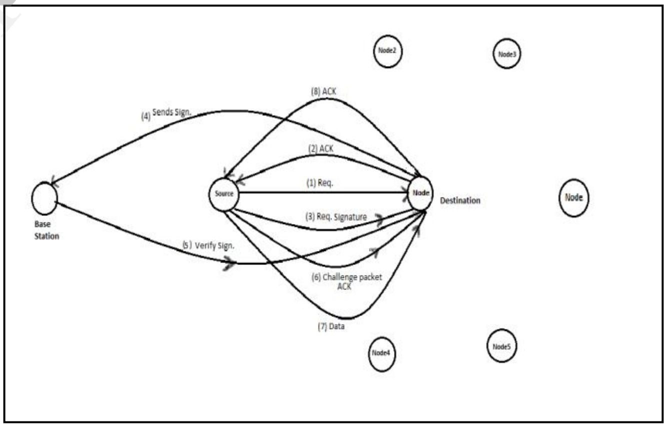

Fig.(2) System control flow diagram

All these above steps are repeated while sending data packet in between any source and the destination node.

VI. PHASES OF THE PROPOSED IDS

The following are the phases with the help of which we can complete our IDS.

a. Network Formation: In this phase the nodes and their ranges are decided
b. Request/ Response: This helps in sending requests and response between the communicating nodes and also the acknowledgements.
c. Base Station Request/ Response: This helps in sending requests and response between the base node and the other node and also the acknowledgements receipt.

d. Data Encryption/ Decryption: It help in encryption or decryption of the data sent through packets.Various algorithms are present for both encryption and decryption. For this we will use the more efficient hybrid cryptography algorithm.

e. Result phase: In this phase we will check for the efficiency of our intrusion detection system on the basis of certain parameters like delay, throughput and energy consumption by the system.

VII. EXPECTED OUTCOME

Proposed system will adopt an intrusion detection system which helps in secure and authentic data transmission with low power consumption, reduced network delays and improved efficiency of MANETs. A more efficient AES technique will be used which provides greater security and more efficient performance in our proposed scheme for the encryption and decryption purpose in proposed system work.

VIII. SUMMARY

In this paper we have studied the various IDS techniques that are used in MANETs to trap the intruders in the network. From this study it is conclude that packet-dropping attack has always been a major threat to the security in MANETs. The functions of such intrusion detection schemes all largely depend on the acknowledgment packets. Hence, the proposed IDS may guarantee that

1. The acknowledgement packets are valid and authentic with more secure data packet transmission.
2. The proposed IDS system will reduce the energy consumption and delays in network with less routing overhead during data packet transmission and also enhance the efficiency of MANETs.

REFERENCES

[1] Ms Pallavi N. Ratnaparkhi, student, Mr.Ravindra D. Kale, Asst. Professor, Dept. of CS/IT G.H. Raisoni Institute of Engineering Technology for Women, Prof. S. S. Patil, Dept. of CT, Priyadarshini Institute of Engineering & Technology, Nagpur, "Review on Intrusion Detection System in Mobile Ad-hoc Networks", in Int. Conf. ICST-2K14, Indapur Pune, Feb. 21-22, 2014.

[2] 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.

[3] Difan Zhang, Linqiang Ge, Rommie Hardy, Wei Yu, Hanlin Zhang, Robert Reschly "On Effective Data Aggregation Techniques In Host-based Intrusion Detection in MANET", The 10th Annual IEEE CCNC- Green Communications and Computations Track, 978-1-4673-3133-3/13, 2013 IEEE.

[4] 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.

[5] 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.

[6] Ms.Sonali P. Botkar, Mrs. Shubhangi R. Chaudhary, "An Enhanced Intrusion detection System using Adaptive Acknowledgment based Algorithm," in World Congress on Information and Communication Technologies, 2011.

[7] A Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, H. Mouftah, "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement", 24th IEEE International Conference on Advanced Information Networking and Applications, 1550-445X IEEE DOI 10.1109/AINA.2010.

[8] Marco Carvalho (Florida Institute for Human and Machine Cognition), "Security in Mobile Ad Hoc Networks," published by the IEEE Computer Society in IEEE Security & Privacy, 1540-7993, 2008

[9] N. Nasser and Y. Chen. "Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network", In Proceedings of IEEE International Conference On Communication, Glasgow, Scotland, June 24 – 28, 2007.

[10] N. Kang, E. Shakshuki andT. Sheltami. "Detecting Misbehaving Nodes in MANETs", The 12th International Conference on Information Integration and Web-based Applications & Services iiWAS2010), ACM, pp. 216-222, November, 8-10, Paris, France, 2007.