INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

INTRUSION DETECTION SYSTEM AGAINST MALICIOUS PACKET DROPPING IN MOBILE AD-HOC NETWORK USING MALICIOUS NODE DETECTION ALGORITHM

MR. SAGAR M. DAMBHARE, DR. S. P. DESHPANDE, DR. V. M. THAKARE

SGBAU, Amravati, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Mobile Ad-hoc Networks (MANET) provides direct peer-to-peer communication between mobile nodes without any infrastructure. During data transfer, it is possible that an attacker may create congestion in network by sending multiple packets that leads to the cause of packet dropping. This paper focuses on different intrusion detection scheme such as collaborative detection, Cooperative baits detection, point detection algorithms, Firecol and Risk-Aware Mitigation. In addition to point detection algorithm a malicious detection algorithm is proposed that detects the malicious node which causes packet loss during transmission from source to destination and improves the network performance.

Keywords: Intrusion detection for MANET, RREQ, RREP, PDN

Corresponding Author: MR. SAGAR M. DAMBHARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Sagar M. Dambhare, IJPRET, 2016; Volume 4 (9): 1076-1086

PAPER-QR CODE

INTRODUCTION

A significant part of the research work has focused on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in fulfilling the requirements of IDS (namely the ability to collect audit data from the network, and apply ID techniques to detect intrusion with a low rate of false positives and an effective response to intrusion).In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

This paper, discusses the intrusion detection methods i.e collaborative detection, Cooperative bait detection, point detection algorithms, Firecol and Risk-Aware Mitigation.In addition to point detection algorithm a proposed method improve the performance of Manet and overcome the problem of packet dropping.

II) BACKGROUND

With respect to the protection strategies for smart meters, it has three major techniques: 1) Intrusion detection system (IDS); 2) remote attestation technologies; and 3) smart meter software modelling. Berthier and Sanders modelled the communication software of a smart meter and introduced a specification-based IDS which can detect the abnormal communications but cannot verify whether they are attacks. Few studies have investigated smart meters' physical components. Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual

misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting Cooperative black hole attacks. Intrusion detection (ID) in MANETs is more complex and challenging than in fixed networks, because of the difficulty in fulfilling the requirements of IDS (namely the ability to collect audit data from the network, and apply ID techniques to detect intrusion with a low rate of false positives and an effective response to intrusion) and because some characteristics of MANETs create operational and implementation complexities. Additional challenges for IDSs in MANETs are as follows:

• MANETs lack concentration points where monitoring and audit data collection can be performed

• MANET routing protocols require nodes to cooperate and act as routers, creating opportunities for attacks

• Due to the nodes' mobility, the network topology is dynamic and unpredictable, making the process of intrusion detection complicated

• IDSs in MANETs are more complex because of the limited computational ability of most of the nodes.

Most recent works aim at countering DDoS attacks by fighting the underlying vector, which is usually the use of botnets. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself , which raises important ethical issues, or to first detect botnet-related malicious activities (attacks, infections, etc.), which may delay the mitigation. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviour's. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

This paper introduces five intrusion detection scheme ie collaborative detection, Cooperative baits detection, point detection algorithms, Firecol and Risk-Aware Mitigation algorithm these are organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III**

discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses comparison of existing method. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III) PREVIOUS WORK DONE

In research literature, many intrusion detection mechanisms have been studied to provide detection against various attacks in MANET and improve the performance of MANET in terms of packet loss, flow control and throughput. Xiaoxue Liu et al. (2015) [1] has proposed a threat model for smart meters. Considering the constrained computation and storage resources of a smart meter, it presents a collaborative intrusion detection mechanism against false data injection attack. It can work regardless of changes in a smart meter's software. Numerical results demonstrate the low cost and effectiveness of proposed intrusion detection mechanism. Jian-Ming Chang et al.(2015) [2] has proposed attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defence architectures. CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery ratio and routing overhead (chosen as performance metrics). Adnan Nadeem et al.(2013) [3] has proposed survey of the main types of attack at the network layer, and it then review intrusion detection and protection mechanisms that have been proposed in the literature. It classify these mechanisms as either point detection algorithms that deal with a single type of attack, or as intrusion detection systems (IDSs) that can deal with a range of attacks. Jerome François et al. (2012) [4] has proposed the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks. Ziming Zhao et al (2012) [5] has proposed a risk-aware response mechanism to systematically cope with the identified routing attacks. Risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, the experiments demonstrate the effectiveness of a approach with the consideration of several performance metrics.

IV) EXISTING METHODOLOGIES

In this section, an efficient intrusion detection mechanism, considering the constrained computation and memory resources of the smart meters. Intrusion detection is the process that monitors the events occurring in a computer system and analyses the events to find out possible incidents. Traditional detecting technologies on malicious codes applied to computers are very power-hungry. This intrusion detection mechanism can achieve collaborative detection of false data injection attack by setting spying domain randomly in physical memory in combination with using secret information and event log. Once the spying domain is modified, illegal reading or writing is identified. The idea of setting spying domain for intrusion detection is inspired by a tool called "Stack Guard" for the buffer overflow attack. Stack Guard inserts a spying word called "Canary" between the return address of memory and the buffer. If the Canary is modified, buffer overflow attack is detected . However, there is a fundamental difference between the spying word Canary and the spying domain proposed in this paper: the location of the Canary is fixed while the spying domain is composed of multiple storage units. The storage units are chosen randomly when legitimate reading or writing occurs in the physical memory of the smart meter. The proposed mechanism has the following requirements.

1) *Secret Information*: Each smart meter has its own secret information and only legitimate procedures can access it. The confidentiality of secret information influences the effectiveness of the intrusion detection mechanism. Hence, it should be updated regularly to resist leakage.

2) *Event Log*: Each smart meter has an event log to record all events including processes of parsing and executing commands to calculate consumption data in the microcontroller, reading/writing in the physical memory, and receiving/sending data via the network interface. The event log is encrypted with the secret information.

3) *Spying Domain:* Every time a legal procedure writes consumption data into the physical memory, several discontinuous storage units are chosen randomly as the spying domain. Then, the hash result of secret information will be written into it. Addresses of spying domain are stored in the event log and the spying domain will be cleared after being read legally. The spying domain is essential for the collaborative intrusion detection mechanism because the spying domain's effectiveness and cost determine the performance of the detection mechanism [1].

CBDS is DSR-based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However,

the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a blackhole attack[2].

Intrusion Detection Systems can be split into three main classes based on the detection approach employed: (1) anomaly-based intrusion detection (ABID), also known as behaviour-based intrusion detection; (2) misuse detection, also known as knowledge-based intrusion detection (KBID); and (3) specification-based intrusion detection (SBID).

1) Anomaly-Based Intrusion Detection*:* Anomaly-based intrusion detection (ABID) systems flag as anomalous observed activities that deviate significantly from the normal profile. ABID systems are also known as behaviour-based intrusion detection, in which the model of normal behaviour of the network is extracted, and then this model is compared with the current behaviour of the network to detect intrusion in the network.

2) Knowledge-Based Intrusion Detection*:* Knowledge based intrusion detection systems maintain a knowledge base that contains signatures or patterns of well-known attacks and looks for these patterns in an attempt to detect them. KBID systems use various methods for constructing and modelling the knowledge for intrusion detection. Some KBID systems use expert systems for intrusion detection. An expert system maintains the knowledge of known attacks in a knowledge base in the form of a set of rules. Captured audit data from a monitoring network are translated into facts and then an inference engine uses these facts and a set of rules in the knowledge base to detect an intrusion in the network

3) Specification-Based Intrusion Detection: Specification-based intrusion detection systems (SBIDs) first explicitly define specifications as a set of constraints. They then use these specifications to monitor the routing protocol operations or network layer operations to detect attacks in the network [3]. Firecol is designed in a way that makes it a service to which customers can subscribe. Participating IPSs along the path to a subscribed customer collaborate (vertical communication) by computing and exchanging *belief scores* on potential attacks. The IPSs form virtual protection rings around the host they protect. The virtual rings use horizontal communication when the degree of a potential attack is high. In this way, the threat is measured based on the overall traffic bandwidth directed to the customer compared to the maximum bandwidth it supports. In addition to detecting flooding DDoS attacks, Firecol also

helps in detecting other flooding scenarios, such as flash crowds, and for botnet-based DDoS attacks [4].

Because of the infrastructure-less architecture of MANET, a risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. The risk aware response mechanism is divided into the following four steps as follows:

Evidence collection: - In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

Risk assessment: - Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

Decision making:-. The adaptive decision module provides a flexible response decision making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfil her goal.

Intrusion response. With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner[5]

V) ANALYSIS AND DISCUSSION

A collaborative intrusion detection mechanism composed of spying domain, event log and secret information for smart meters. This intrusion detection mechanism focuses on the false data injection attack and can work regardless of changes in software. Illustrative results have shown the effectiveness and low cost of the proposed scheme and suggested the key parameter determination. An interesting future topic is the reliable and effective updating mechanisms for smart meters' secret information [1].

A new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative black hole attacks. The simulation results revealed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. As future work, it intend to 1) investigate the feasibility of adjusting CBDS approach to address other types of collaborative attacks on MANETs and to 2) investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants[2].

However, it shows that intruders often find new ways to attack and cause damage to computer systems and networks. Therefore, it consider that enabling a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities (attacks) is an important and potentially fruitful area of future research [3].
FireCol, a scalable solution for the early detection of flooding DDoS attacks. Experiments showed good performance and robustness of *FireCol* and highlighted good practices for its configuration. Also, the analysis of FireCol demonstrated its light computational as well as communication overhead [4].

A risk-aware response solution for mitigating MANET routing attacks. Based on several metrics, it also investigated the performance and practicality of approach and the experiment results clearly demonstrated the effectiveness and scalability of risk aware approach. Based on the promising results it would further seek more systematic way to accommodate node reputation and attack frequency in the adaptive decision model [5].

IDS Scheme	Advantage	Disadvantage
CIDM	It can achieve collaborative detection of false data injection attack by setting spying domain randomly in physical memory in combination with using secret information and event log.	When the attackers are powerful ones who may have analyzed a smart meter's software and stolen the secret information in advance.
CBDA	Cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch grayhole /collaborative blackhole attacks	Malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead.

Point detection algorithm	Point detection algorithms as those that can detect a single category of network layer attacks and general intrusion detection systems (IDSs as those that can detect a range of attack types.	One needs to have confidence that there are no attacks taking place during training period of detection system. Intruders often find new ways to attack and cause damage to computer systems and networks.
Firecol	It shares information between different network nodes to mitigate efficiently flooding attacks,	FireCol does not allows the coexistence of multiple virtual protection rings for multiple Customers across the different set of IPSs.
Risk-Aware Mitigation	Risk-aware approaches are Introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way.	It work fails to take advantage of IDS alerts and simple isolation may cause unexpected network partition

TABLE 1: Comparisons between different Intrusion detection Mechanism

VI) PROPOSED METHODOLOGY

The proposed method introduced Malicious Node Detection algorithm that detects malicious node which causes packet dropping in Manet. This technique discards the malicious node in the network.

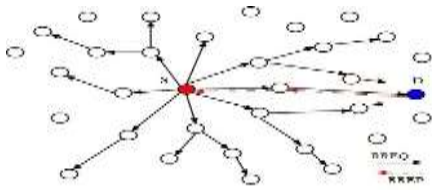

Fig 1.Process of the route discovery between nodes S and D.

Fig 1 shows the route discovery between source and destination. The source broadcast RREQ message to all nodes in the network if it receives RREP then it is a destination. The path discovery node maintains the path details from each node to destination .If a Node is sending packet through various links then it will increase the congestion in network so that it may lead to drop the packets. The Malicious Node detection algorithm is as follows.

Malicious Node Detection Algorithm

1. Create a Path Discovery Node.

2. Broadcast RREQ massage packet to find the path of intermediate nodes and shortest stable path connectivity.

3. If it is destination then sends RREP packet to source otherwise broadcast to neighbouring nodes

4. If node sends packet through more than one path

Then Malicious Node

Otherwise

Normal Node

5. End if

OUTCOME POSSIBLE RESULT

The proposed Malicious Node Detection Algorithm will successfully remove malicious node which causes packet dropping.

VII) CONCLUSION

This paper focused on the intrusion detection scheme i.e. collaborative detection, Cooperative bait detection, point detection algorithms, Firecol and Risk-Aware Mitigation. This approach provide malicious node detection algorithm to detect malicious node which causes packet dropping.

VIII) FUTURE SCOPE

As future work, it intends to investigate the feasibility of adjusting our malicious node detection approach to address other types of packet dropping attacks on MANETs.

REFERENCES

1. Xiaoxue Liu Peidong Zhu, Yan Zhang, and Kan Chen," A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure", IEEE TRANSACTIONS ON SMART GRID, VOL. 6, NO. 5, SEPTEMBER 2015.

2. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai ," Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015

3. Adnan Nadeem, Michael P. Howarth," A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013.

4. Jérôme François, Issam Aib, and Raouf Boutaba,"FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, DECEMBER 2012.

5. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu , "Risk-Aware Mitigation for MANET Routing Attack IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO.MARCH/APRIL2012.