International Journal of Advanced Computer Technology
ISSN: 2319-7900 www.ijact.org Volume-X, Issue-I, February 2021

Collaborative Profile Assessment to Secure MANET by DDOS Attack

Vinita Kushwaha[1], Kailash Kumar Patel[2], Prashant Richariya[3]
Computer Science & Engineering
Technocrats Institute of Technology-Advance, Bhopal, India
[1]Vinitakushwaha97@gmail.com, [2]Patelkailashkumar@gmail.com, [3]prashant1579@gmail.com

Abstract— In the Mobile Ad-hoc Network, nodes bind together in the centralised authority's absence because reliability is one of the main challenges. The MANETS protective architecture provides some consequential problems due to the specific features of MANETS. The DDoS attack in the network is not quickly detectable. A management infrastructure that guarantees extensive security and the required network performance from attacks must be developed to overcome the barriers. Direct methods cannot be found successfully in mobile ad hoc networks in which network topology differs animatedly. Different DDoS security systems boost the network's output in front of an attacker to deactivate mismanagement, like NTRS. In this study, the Distributed Profile Evaluation Mechanism (DPEAP) DDoS Attack Effect in the Network proposes that compromise packets tossed out of the network beyond the network's capacity. The NTRS was a modern methodology in the study, and the DPEAP suggested is a new technique. The DPEAP identifies the attacker's behaviour by matching an attacker's profile with the ordinary nodes on the network, provided that the Node Profile is regular in the foaming of the proper network data delivery. The DPEAP then declare that the attacker's network has no hazard. In contrast with NTRS in MANET, the DPEAP method is stable and efficient.

Keywords— Detection, Security, DDOS, MANET, DPEAP, NTRS, AODV

I. INTRODUCTION

The Mobile Ad-hoc Network (MANET) is made up of a temporary network, without the need for central management or traditional support equipment available in a conventional network, thereby forming an infrastructure-free network [1, 2]. Intuitively, intrusions in an information system are the operations that violate the system's security protocol, and the mechanism used to classify intrusions is intrusion detection. For about 20 years, intrusion detection has been researched. It is founded on the premise that an attacker's behaviour varies greatly from that of a legal person and that several illegal acts observable. As the second level of protection that defends information infrastructure, intrusion detection systems (IDSs) are typically implemented along with other protective security measures, such as access control and authentication. There are a variety of reasons for making intrusion detection a necessary aspect of the whole defence mechanism. First, without protection in mind, many conventional systems and applications have been developed.

In other instances, systems and applications have been designed to run in a particular context, and when implemented in the current environment, they may become vulnerable. (For example, when it is inaccessible, a device may be completely safe, but it becomes susceptible when connected to the Internet.) Intrusion detection provides a way to recognise and thereby facilitate responses to attacks against these systems. Second, operating systems and applications have design vulnerabilities or glitches that an attacker may exploit to target the systems or applications due to the shortcomings of information technology and software engineering experience. Some prevention measures cannot be as successful as planned (e.g., firewalls).

Detection of attack complements these defensive measures to increase the protection of the device. Also, even though preventive protection measures can effectively secure information networks, it is desirable to know what intrusions have arisen or are occurring to identify the security challenges and risks and, therefore, be properly prepared for possible attacks.

IDSs, despite their significance, are not substitutes for protective security measures, such as access management and authentication. IDSs themselves will, of course, not have appropriate securities for information systems. If an attacker erases all the data in an information system, detecting the attacks not reduce the damage at all as a drastic example. Thus, as part of a robust defence framework, IDSs should be deployed along with other preventive protection measures.

Techniques for intrusion detection are generally divided into two methods: detecting irregularities and detecting misuse [3-6].

Detection of deviations is based on a subject's normal behaviour (e.g., a person or a system); any action that deviates significantly from normal behaviour is considered intrusive. In terms of the features of known threats or device vulnerabilities, exploitation detection captures intrusions; any behaviour that conforms to the pattern of a known threat or susceptibility is called invasive.

Alternatively, IDSs can be classified into host-based IDSs, distributed IDSs and network-based IDSs based on the source of the audit information used by each IDS. Host-based IDSs gather audit data from host audit trails and usually aims at detecting attacks on a single host; distributed IDSs collect audit data from multiple hosts and potentially from the networks linking hosts for attacking, including several hosts. Networked IDSs use network traffic as a data auditing point, reducing the burden on hosts of typically normal computing resources.

II. OBJECTIVE

In a mobile ad hoc network, node mobility and route fluctuation promote the network by various attacks such as routing, rushing, and resource consumption, which benefited the attacker. Out of those attack, rushing attacks is very harmful because it captures the legitimate nodes and trained to illegitimate those nodes and completely crush the overall network and increase very high congestion. So that in this dissertation, our general objective to prevent the network by a distributed denial-of-service attack is a type of rushing attack. In favour of fulfilling the requirement of a general objective, some specific objectives are designed.

1. Investigate existing rushing attack and their symptoms to utilise their behaviour for our research work in further prevention.
2. Design and develop distributed profile evaluation-based security mechanism which secures the network from distributed denial of service attack.
3. They are blocking unwanted message flooding to minimising the network overhead.
4. Analysis of the impact of the proposed security mechanism concerning network parameters and comparative study from existing neighbouring trust-based security methods.

III. LITERATURE SURVEY

Anuj Rana *et al.* [7] "EMAODV: a technique to prevent collaborative Attacks in MANETs" In this title, a joint attack on Manets in Manets algorithm is discussed. In this title. The most difficult issue of multiple vulnerabilities in MANETs is the safety or secure touch. As an invalidation of authorisation functions, network environment less infrastructure, node motions dynamically randomise bugs or special features that make MANETs vulnerable to several assaults. Mutual threats have a harder effect than human attacks on MANET. The increasing need to use MANETs has resulted, but even a lack of fully secure protocols requires it to be free of communications issues due to various protocols and reliable algorithms.

Raksha Upadhyay, *et al.* [8] "DDOS Attack Aware DSR Routing Protocol in WSN" Open Design opens up to external attacks in this word. Wireless Sensor Network (WSN). Many security risks, such as the denial of service, black hole, sinkhole, may impair the network's performance. Distributed Denial-of-Service attacks (DDOS) are defined as attacks initiated by various malicious organisations at a node or group of nodes. In this profession, we suggest a solution to prevent WSN from using dynamic source routing from a DDOS attack (DSR). Energy from the nodes involved was used for attack detection and prevention. The Qualnet 5.2 simulator used to implement the approach proposed.

Muhammad Imran *et al.* [9] "Analysis of Detection Features for Wormhole Attacks in MANETs" in this title, based on their shortcomings and features critical in detecting wormhole attacks MANETs, we thoroughly research this current system. We address a recent method focused on two Bayesian classification methods.

M. Rmayti *et al.* [10] "Denial of Service (DoS) attacks detection in MANETs through statistical models" Several experiments using the NS2 simulator have been conducted. Our filters indicate that with a low level of false warnings, purposely falling packets can be completely observed.

Gising Kim *et al.* [11] "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection" This title proposes a new methodology for hybrid intrusion detection that hierarchically combines a paradigm for misuse detection and an anomaly detection model into a framework for decomposition. Second, based on the C4.5 decision tree algorithm, the incorrect usage detection model is constructed, and then the usual training data is broken down using the model into smaller subsets. Next, for the decomposed subsets, several one-class SVM models are generated.

Adnan Nadeem, *et al.* [12] "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" This title addresses core types of network layer attack and the potential intrusion prevention and protection mechanisms of the literature. Furthermore, we define these mechanisms as algorithms for spot detection that deal with an attack or as (IDSs), which can cope with several attacks. Yadav et al. [13, 14] have proposed improving the throughput, stability, and lifetime of sensor network based on cluster network and also provide a trust factor of the network using trust value.

Muamer N. Mohammad *et al.* [15] "A Novel Intrusion Detection System by using Intelligent Data Mining in Weka Environment" In this title, Weka presents and applies an improved approach to intrusion detection system focused on the combination of data mining and an expert system. The taxonomy consists of a classification of the theory of detection and some elements of the WEKA method of detecting intrusions, such as open-source data mining. Combining methods can provide IDS systems with improved performance and make identification more efficient.

IV. PROPOSED ARCHITECTURE

This section designs a working architecture of the proposed distributed security system, which detect and prevent the network from distributed denial of service attack. In this architecture, deploy the mobile node and select some node as the source and their respective receivers. Source node initiates to call routing protocol, search the route from source to receiver node, and perform data communication. Meanwhile, some attacker node generates the unwanted packet and floods these packets in high rate, increasing network congestion and consuming its resources. In this architecture, the proposed security system detects and prevents the network from a DDOS attack on the profile evaluation method's bases and takes the collaborative decision to block the attack node and provide secure communication permanently.

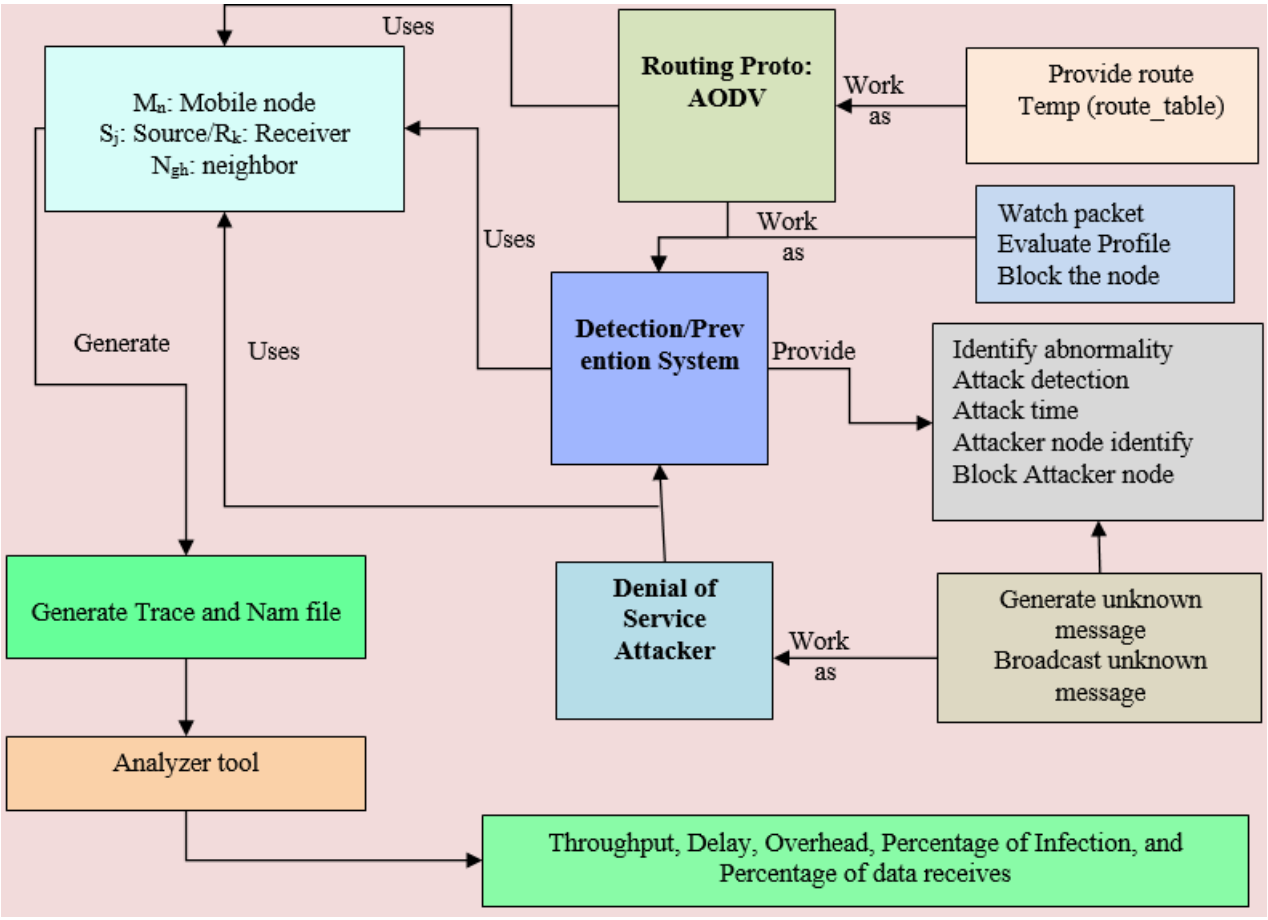

Figure: 4.1: Proposed Distributed Prevention Architecture

V. Proposed DPEAP Scheme

Distributed denial of service (DDOS) is a kind of attack targeting to gain the network resource and unwanted flood packet in the network to increase congestion. DDOS attack spoof some security system by routing discovery time not detected as an attacker. During data communication, it is illegitimate lead work to flood a higher volume of unwanted junk message into the network and damage a complete system that goes to a heavy congestion state. Some researchers detect the DDOS attack by the various technologies in the existing security system, but they cannot completely prevent DDOS attack in MANET. This dissertation develops a suitable technique that completely secures the network by a DDOS attack. Our proposed distributed profile evaluation technique secures the network through a DDOS attack.

In this technique, the M mobile node in a network out of M node N < M number of mobile nodes contains a security system that can trace another node in the network and neighbour. The proposed security system uses route protocol ad-hoc on-demand distance vector routing (AODV), which is dynamic routing suitable for ad hoc communication and established the route between source to destination with a multi-hop link disjoint path. While the route is established and the source wants to transmit the data by legitimated transport layer protocol, the attacker is in active mode and generates huge amounts of junk message during a short period. The generated junk message spread via the neighbour Connected node and lunch the DDOS attack, which consumes the network resource via flooding unwanted data. But our proposed distributed security system deploys in a random manner, which is watching the network's behaviour in every discrete event of time—the security system work into two steps detection and collaborative decision-based prevention.

In the detection phase, the security system individual executes and monitors the respective neighbours' behaviour and watches every activity performed by its neighbour. That activity store in a temporary manner in the security system and classified into normal data and suspicious data. All suspicious data also classify by into two categories, such as network relative issue or unmatched protocol issue. Simultaneously, the detection system found suspicious data as a network relative issue than instantly call to a network management protocol to take further action to resolve those problems. Another side of the detection system is unmatched protocol. It assumes the behaviour as an attack packet and records their identity for further decision. The reason for unmatched data is (rush packet in limited time, unknown protocol use, packet drop without network-dependent reason). Security system detects neighbour node as an attacker than its temporary block that node and simultaneously the multiple security systems those watch similar neighbour node, collaboratively decide to permanently block or give other chance to behave as a genuine

protocol in further communication. It depends on their activity, per unit time, the number of junk packet generation and total node captured by an attacker node. The proposed distributed system secures the network by a distributed denial-of-service attack and provides reliable communication in network parameters such as throughput, packet delivery ratio, overhead and minimum delay.

VI. Simulation Parameters

Table 1 shows the simulation parameter, and based on that, all three scenarios are designed. The DDoS Attack and recovery through NTRS and propose DPEAP scheme having the same scenario of communication. The routing protocols, grid layout, number of nodes, Antenna, and others are also mentioned to measure all three scenarios' performance.

Table 1 Network Input Parameters

Parameters	Configuration Value
Routing Protocol	AODV
Simulation Area	800m*800m
Network Type	MANET
Number of Nodes	50
Physical Medium	Wireless, 802.11
Mobility Speed	Random
Mobility Model	Random Waypoint
Attack Type	DDoS
Secure Protocol	DPEAP
Simulation Time (Sec)	100Sec
Transmission Range	550m
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground

VII. Simulation result

A. Data Send Analysis

This analysis compares the result in terms of data sending by the genuine sender nodes. In the simulation, take the fifty-node environment and create the sender node in three different scenarios. In the denial-of-service attack source node sends the data in nearly 4343 packets. The data were sending 7010 packets, and our proposed approach of the data sending is higher than the existing approach in the existing system. The result shows that the proposed system is more secure as compare to the existing NTRS protocol.

B. Data Receive Analysis

The receiver's data is an important parameter for communication because it relates to the percentage of data receiving. The result shows the number of packets receives by the genuine receiver in the network. The result concludes that only 3114 packets receive a denial of service attack cases, which is very poor because of the attacker nodes' data drop. The data receive 10008 packets in proposed security, which show that our effective receiving service to the end receiver node.

C. Summarise Performance Analysis

Table 3 represent the cumulative output of the network. It reflects all the summery efficiency metrics in the exact figure foam, which indicates how many packets are sent, received and lost on the network in case of NTRS routing, attack and DPEAP.

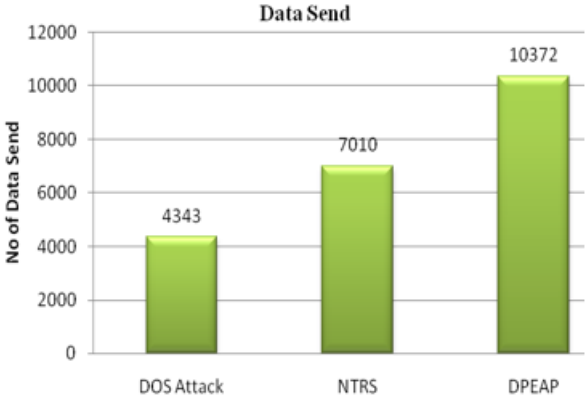

Figure 2: Data Send Analysis

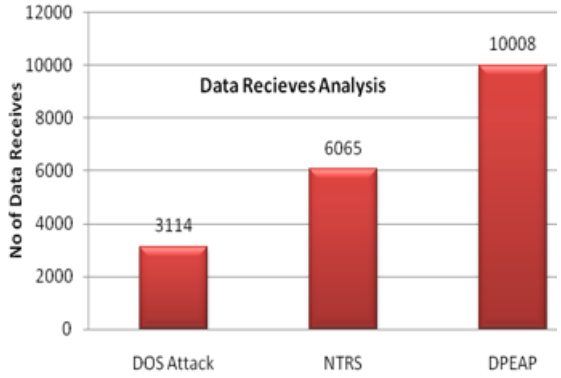

Figure 2: Data Receives Analysis

Table 2 Summarize Analysis of Network

Parameters	DOS Attack	NTRS	DPEAP
Packet Sends	4343	7010	10372
Packet Receives	3114	6065	10008
Packet Drop	1229	945	364
PDR (%)	71.70	86.52	96.49
NRL	63.94	1.36	0.54
Average Throughput [Kbps]	797.18	1552.64	2715.77
Average Delay [ms]	1.05	0.53	0.41

VIII. Conclusion and Future Scope

In MANET, nodes continuously share network knowledge, But the information breaks into several numbers of packets flooded into the network, in which case the network is affected by the DDoS attack. The proposed structure removes the need for a centralised authority, which is not technically in the wireless sensor network due to its self-organising existence. When the route is established and the source wants to transmit the data, the attacker is in active mode and generates a huge amount of junk message during a short period. Simultaneously, the detection system

found suspicious data as a network relative issue than instantly call to a network management protocol to take further action to resolve those problems. The attacker has compromised 38 per cent of the network performance but is still impaired by the remaining network performance. The packet dropping is almost one-third of the previous scheme. The PDR is 10% more than the previous scheme, and overhead is almost half compared to the previous NTRS scheme. The proposed DPEAP scheme produces improved outcomes in the case of a DDoS intruder. The proposed security system uses route protocol ad-hoc on-demand distance vector routing (AODV), which is dynamic routing suitable for ad hoc communication and established the route between source to destination with multi-hop link disjoint path. Another side of the detection system found as the unmatched protocol is that it assumes the behaviour as attacker packet and records their identity for further decision. The performance of the proposal DPEPP scheme was better as compared to the NTRS scheme. In the future, measures the performance of grey hole attack and black hole attack. Other methods such as packet capture, false path forwarding, swapping source and destination addresses used in the future for secure communication in MANET

REFERENCES

[1] M.M. Lehmus, Requirements of ad hoc network protocols, Technical report, Electrical Engineering, Helsinki University of Technology, May 2000.

[2] N. Asokan, P. Ginzboorg, Key Agreement in ad hoc Networks, Computer Communications 23 (17), pp.1627-163, 2000.

[3] G. C. Siva Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.

[4] Dokurer, Semih." Simulation of Blackhole Attack in Wireless Ad-hoc Networks". Master's thesis, Atılım University, September 2006.

[5] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.

[6] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communication, 14 (5), pp. 85-91, 2007.

[7] Anuj Rana, Vinay Rana, Sandeep Gupta "EMAODV: a technique to prevent collaborative Attacks in MANETs" Elsevier procedia computer science 70 (2015) 137 – 145.

[8] Raksha Upadhyay, Uma Rathore Bhatt, Harendra Tripathi, "DDOS Attack Aware DSR Routing Protocol in WSN" Elsevier International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.

[9] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad "Analysis of Detection Features for Wormhole Attacks in MANETs" Elsevier Procedia Computer Science 56 (2015) 384 – 390.

[10] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, "Denial of Service (DoS) attack detection in MANETs through statistical models" 978-1-4799-5490-2/14/$31.00 ©2014 IEEE.

[11] Gisung Kim, Seungmin Lee, Sehun Kim, "A novel hybrid intrusion detection method was integrating anomaly detection with misuse detection" Elsevier Expert Systems with Applications 41 (2014) 1690–1700.

[12] Adnan Nadeem, Member, IEEE and Michael P. Howarth "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE communications surveys, accepted for publication 1553-877, 2013IEEE.

[13] Yadav, Amrendra Singh, et al. "Increasing Efficiency of Sensor Nodes by Clustering in Section Based Hybrid Routing Protocol with Artificial Bee Colony." Procedia Computer Science 171 (2020): 887-896.

[14] Yadav, Amrendra Singh, Shivani Agrawal, and Dharmender Singh Kushwaha. "Distributed Ledger Technology based Land Transaction System with Trusted Nodes Consensus Mechanism." Journal of King Saud University-Computer and Information Sciences (2021).

[15] Muamer N. Mohammad, Norrozila Sulaiman, Osama Abdulkarim Muhsin, "A Novel Intrusion Detection System" using Intelligent Data Mining in Weka Environment" ELSEVIER Procedia Computer Science 3 (2011) 1237–1242.