International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

A Survey on Data Intrusion schemes used in MANET

Basappa Birajdar[1], A. N. Pimpale[2], Nilima Nikam[3]

[1] M. E Student, Dept. of CE ,YTIET, Karjat , Maharashtra, India

[2] Lecturer, Dept. of ExTc ,YTP, Karjat, Maharashtra, India

[3] Nilima Nikam,HOD, Dept. of CE,YTIET, Karjat, Maharashtra, India

---

Abstract - *Mobile Ad hoc networks gained popularity because of flexibility in their architecture. MANET networks found correlated applications with WSN. Due to dynamic architecture of MANET, it had gone through many problems in data intrusion. This paper reviews some problem definitions in data intrusion of MANET. Also reviewed some proposed solutions in problem definitions of data intrusion. Proposed method introduces RWD for efficient detection eliminating detection engines in WSN.*

Key Words: **MANET, RWD, Intrusion Detection Schemes (IDS).**

1. INTRODUCTION

Due to use of wireless sensors, mobile ad hoc networks are more susceptible to attacks. Security in data is one of the prime issues. Intrusions are actions to compromise integrity, confidentiality with available resources [1]. Intrusion detection systems are mainly classified in terms of their data collection, detection & response. Basically three techniques had adapted in literature for data intrusion.

1) Anomaly-based intrusion detection
2) Misuse-based intrusion detection
3) Specification based intrusion detection

MANET networks are characterized by some of the problematic characteristics such as lack of central point, mobility in wireless network, bandwidth requirement, line of sight problem, & limited resources [2].

Nevertheless, it is very difficult to design a once-for-all detection model. Some proposed intrusion detection schemes to overcome these problems are discussed below.

1.1 Distributed and Cooperative IDS

This was the first IDS proposed by Zhang & Lee. This intrusion detection mechanism is based on reliable exchange of network events and active cooperation between the participating nodes. In this scheme every node having IDS detect local intrusion & co-operate with neighbor node. Absence of centralized node makes this scheme traffic concentrated [3].
Routing Protocol Analyzer (RPA) & distributed Intrusion Detection Engine (DIDE) has implemented to observe local aggregate traffic considering local mobility.

1.2 Cooperative IDS using Cross-Feature Analysis in MANETs

This scheme based on data mining technique. It automatically constructs an anomaly detection model. Model uses cross feature analysis & define rules to detect attacks or attackers. Every node analyzed & compared with its predicted values. Average of node count or its probabilities calculated for anomalies [4]. Different algorithms such as C4.5, Ripper, and NBC were instigated to calculate PDF. Cluster based IDS architecture proposed for cluster heads. Equal service time assigned to all cluster heads. Statistic based analysis is also one of the solution.

1.3 Zone-Based Intrusion Detection System

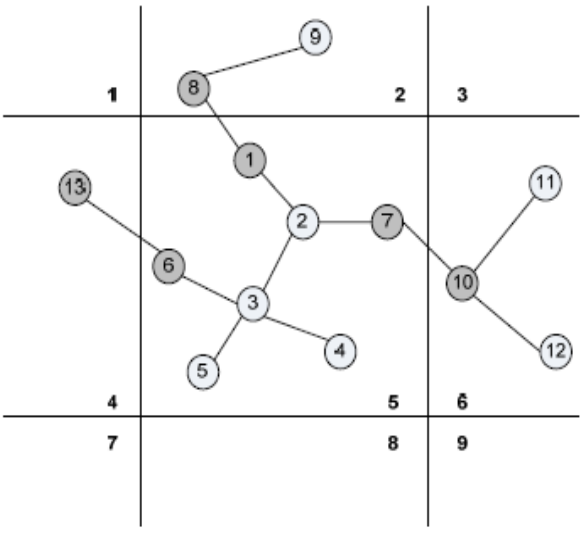

Fig. 1 Zone based IDS

Overlapping of zone based traffic avoided by division of geographic partitioning. Partition classified as intra zone & inter zone as shown in figure 1. Intra zone nodes perform aggregation & correlation while inter zone nodes give false alarm rate with final decision. MANET Intrusion Detection Message Exchange Format defines the format of information ex-change between IDS agents. It also considers mobility based on changes of node's with neighbors. But the drawback of this method is it also causes detection and response latency even when there is enough evidence on local nodes [5].

1.4 General Cooperative Intrusion Detection Architecture

This is cooperative and dynamic hierarchical IDS architecture. This scheme uses multiple-layered clustering in intrusion detected nodes.

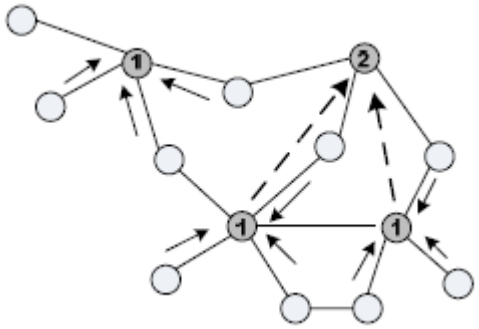

Fig. 2 General cooperative IDS

The data flow controlled between the level nodes to its cluster heads in upward or downward direction. The dynamic hierarchical data is in upward direction while the command flow is in downward direction. Applicability of such architecture found in military applications. Limitation of such architecture is high-cost maintenance of the architecture under high mobility [4, 5].

1.5 Intrusion Detection Using Multiple Sensors

Use of multiple sensors increased now days in IDS because of benefit of lower bandwidth. It is based on three mobile agent classes' i.e. monitoring, decision making & action taking.

Voting performed for cluster heads based on their connectivity. Cluster heads having their individual responsibility of locality, decision making & detection. Limitation of this scheme is that as number of node hoping increases efficiency & security decreases. Method is not that much efficient for real time data intrusion [6].

1.6 Specification-Based IDS for AODV

In this IDS scheme Network Monitor (NM) assumed to cover all nodes & their properties like MAC address, IP etc. known to NM. Nodes in the broadcasting range, broadcasts secure massages. I f they do not responds it causes some serious problem. Finite state machines (FSM) for nodes requests rout of forwarding massage & replied massages monitored. Conditions like frequent high mobility are tough to detect. To overcome this problem path tracing is preferred. This scheme is applicable to both known & unknown ID attacks [7].

1.7 Distributed Evidence-driven Message Exchanging ID Model (DEMEM)

Every node monitored by neighboring hopping node. Evidence driven massage exchanging format decided to detect intrusion in between two hopping nodes. If new evidence found then nodes send massages by introduction of a new intrusion detection layer in between IP layer & Routing layer.

Multipoint relay to reduce flooding of broadcasting massages & topology control are two advancements implemented over this scheme. When a detector detects an intrusion, it automatically seeks to correct the falsified data. Applicability of DEMEM found in reactive protocols which are addressed over proactive protocols [4, 7].

2. Proposed method (RWD method)

The proposed method works on the basis of RWD (Random Walker Detection).

Proposed method basically works on effectiveness of detection engine at each node. It is stochastic process, which represents a path of random successive steps. At each visiting node RWD deploys multi-layer specification based intrusion detection engine, which monitors the protocols and operations at the transport, data link and network layer. Existing system tries to prevent the system from attacker and also find the attack in the network. RDS will detect the attacks on each node or network. If any node found to be malicious in transmission of data then packet data routed from another path. Such method does not block packets & hence conjunction time reduces.

Algorithm implemented in fallowing modules & their outcomes discussed below in short. RWD specified in transport layer, network layer, & data link layer. Detection engines excluded from RWD so not discussed here in detail.

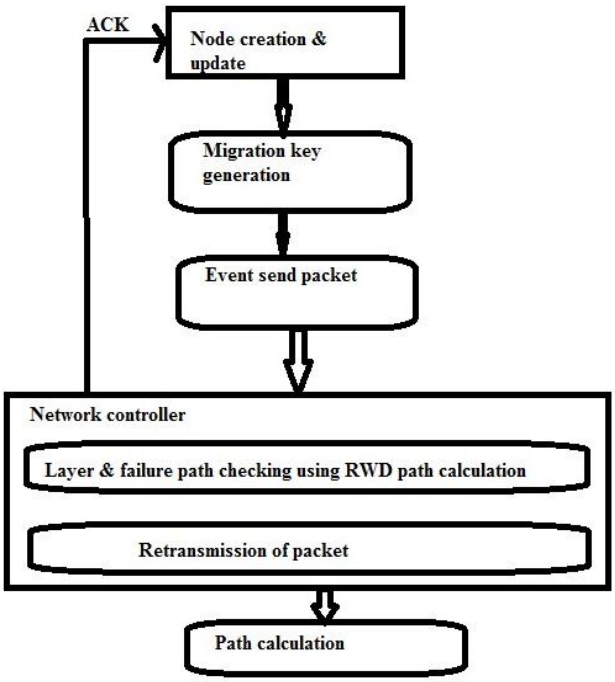

Fig.3 RWD method for path calculation

1. Node creation keeps tracks of suspicious node in encrypted form.
2. Key generation performs secure communication between node & network.
3. Event is nothing but communication or transmission of encrypted massage from source to destination.
4. Network controller module having role of monitoring specific node for its malicious behavior. If found to be malicious then new path found out using RWD.
5. Rerouting needed to overcome the drawbacks like lack of infrastructure, power limitations,

Algorithm used here is advanced encryption standard (AES).

3. CONCLUSIONS

Dynamic characteristic of MANET produces data intrusion in network. Random walk detector (RWD) works well on three layers i.e. data link layer, network layer & transport layer. Most critical type of attacks can be detected by RWD. Retransmission & rerouting mechanism in RWD fix MANET infrastructure. Power limitations overcome. Encryption & key generation make RWD more secure than other algorithms hence efficiency improved. Advanced encryption standard implanted in RWD.

REFERENCES

1. Christoforos Panos "A Novel Intrusion Detection System for MANETs" IEEE Wireless Communications Surveys, Vol. 11, No 1. 2014, pp. 38–47.
2. Anantvalee T, Wu J (2006) "A Survey on Intrusion Detection in Mobile Ad Hoc Networks". Wirel/Mobil Netw Secur, Springer:170-196
3. Y. Ping, J. Xinghao, W. Yue, and L.Ning, " Distributed intrusion detection for mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 19, no. 4, pp. 851–859, 2008.
4. Huang Y, Fan W et al (2003) Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies. *In Proc of 23rd IEEE Int Conf on Distrib Comput Syst (ICDCS):*478-487
5. M. Joa-Ng and I. Lu, "A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks," in IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, Aug., 1999, pp. 1415-1425.
6. Zhang Y, Lee W "Intrusion Detection Techniques for Mobile Wireless Networks. " Wireless Network : 545-556
7. Uppuluri P, Sekar R " Experiences with Specification-based Intrusion Detection" In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189
8. Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks", IEEE Journals on selected Areas in Communications, Vol 28, No 5.
9. Huang Y, Lee W "A Cooperative Intrusion Detection System for Ad Hoc Networks." In Proc of the 1st ACM Workshop on Secur of Ad Hoc and Sens Netw:135-147
10. Sevil Şen, John A. Clark "Intrusion detection in mobile ad hoc networks" Guide to wireless ad hoc networks, 427-454.

BIOGRAPHIES

Basappa Birajdar currently pursuing M. E. in YTIET Karjat, Maharastra (India) in computer Engineering. He has 5 years of programming experience in Java & Advanced Java level.

Mr. A. N. Pimpale received M. Tech degree in digital communication from RGPV Bhopal (India). Currently he is working as a lecturer in YTP (ExTc) Karjat, Maharashtra (India).