A Recent Analysis of Intrusion Detection and Prevention System for Protecting Range of Attack using Data Gathering Technique in MANET

R.Arunkumar
M.E CSE
K.S.R College of Engineering
Tiruchengode, Tamil Nadu

Mrs.A.Annalakshmi
Associate Professor
K.S.R College of Engineering
Tiruchengode, Tamil Nadu

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a mobile and multi-hop autonomous operation of wireless network. Collection of wireless mobile nodes way of forms a temporary network without using any pre-existing infrastructures. Intrusion Detection & Prevention System (IDPS) is one of the defence mechanisms to protect MANET against variety of attacks due to the dynamic topology, lack of centralized control, limited physical security and energy constrained operations. This paper aims to focus on monitored the most prominent techniques of IDS approach for determining under the conditions of critical nodes and also trigger & compare the recent Intrusion Detection mechanism based on their architecture and data gathering techniques.

General Terms

Enhanced Adaptive ACKnowledgment; Vehicular Ad-hoc Network; k-Nearest Neighbors.

Keywords

Intrusion Detection and Prevention; Mobile Ad hoc Networks; Watchdog; CPDOD; Intrusion detection system; CP-KNN; Intrusion Detection & Prevention System.

1. INTRODUCTION

At present two deviations of wireless mobile networks node. The primary one is known as infrastructure networks that contains fixed and wired gateways. The next type of mobile wireless network is the infrastructureless mobile network generally known as an ad-hoc network. Infrastructure less mobile node has no fixed routers; all nodes are moves and connected dynamically in an arbitrary manner. Function on node act as routers as well as a host which discovers and maintains routes to other nodes over network radio range communicates directly via wireless links.

An Intrusion Detection System (IDS) is a device or software applications for monitoring network traffic, suspicious activity if any deviation occurs against normal behavior, then give alerts the system or network administrator. An IDS [17] is software that automates the intrusion detection process. The primary responsibility of IDS is to detect unwanted and malicious activities. Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. This paper proposed survey of different Intrusion Detection System for MANET based on their architecture and data gathering techniques.

The reminder of this paper is organized as follows. Section 2 describes the An Overview on MANET Related Work. Section 3 Background Methodologies of IDS for MANET. Section 4 Evaluation Metrics for MANET Routing Protocols. Section 5 Researches Achievement in Comparative evaluation of Various IDS Technique for MANET. Section 6 Summaries of Reviewed Ids for Detecting Misbehaving Nodes. Finally, Section 7 we summarize our Conclusion and Future Research work.

2. AN OVERVIEW ON MANET RELATED WORK

A Mobile Ad-hoc network [4] is a wireless ad-hoc network which is used to each node is eagerly to forward data or exchange information to other nodes. It is a self configuring dynamic network of mobile devices connected by wireless links in a hostile environment without any pre-fixed infrastructure. Most challengeable security design of MANET includes an open decentralized peer-to-peer architecture, a wireless shared medium and a highly dynamic topology by the malicious attackers. The protecting in a MANET is constituted by intrusion prevention systems like cryptography and authorization and implementation not always possible due to the limitations that some nodes may present.

MANET consists of two types: Vehicular Ad-hoc Network (VANET) is used for communication among vehicles and between vehicles and roadside equipment. Internet Based Mobile Ad-hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet gateway nodes.

2.1 MANET Features

a) **Light-weight Autonomous terminal:** A function of mobile node may act as both host/router.

b) **Distributed Operations:** Because there is no fixed network for control and management operations are distributed among the terminals.

c) **Multi-hop routing:** Delivering packets via one or more nodes.

d) **Dynamic network topology:** As the network varies rapidly, the movable nodes dynamically establish routing among themselves.

2.2 Security Issues of MANET

A major issue in Mobile ad-hoc network is "**SECURITY**" enforcement [1]. Since, MANET are easily vulnerable because due to absence of centralized control, unguarded dynamic topology routing medium, ad hoc networks do not have a well-defined boundary area, and thus, mechanisms such as firewalls are not applicable for lagging of security and reliability Quality of Service.

Two approaches for protecting mobile ad-hoc networks.

a) **Reactive Approach:** Looking for detecting security threats and reacts accordingly.

b) **Proactive Approach:** It's trying to attempts for prevent an attacker from launching attacks through various cryptographic techniques.

2.3 Classification of Attacks on MANET

Many types of attacks can be performed over a MANET network as see Figure 1. In this section, we analysis those types of attacks according to the various MANET models with the help of IDS Technique to prevent and expose the normal operation of the network against a mixture of attack.

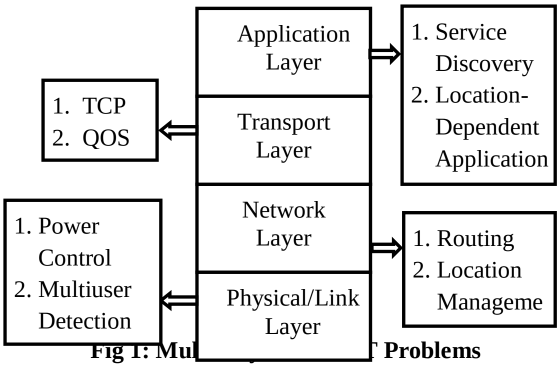

Fig 1: Mul T Problems

3. BACKGROUND METHODOLOGIES OF IDS FOR MANET

3.1 IDS Process in MANET

An intrusion detection system (IDS) [5] monitors network traffic and monitors for suspicious activity and alerts (like a burglar alarm) the system or network administrator. In a few cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. Intrusion detection is a necessity in any high-survivability network.

Intrusion prevention procedures are inserted into a network; there are always some weak links that can be broken. It contributes to improve the security policies used to detect the possible threats and points of failure in the network. Two aspects for security is [5],

a) Alert the network.

b) Take direct reactive and preventive measures to protect the network.

3.2 IDS Structure

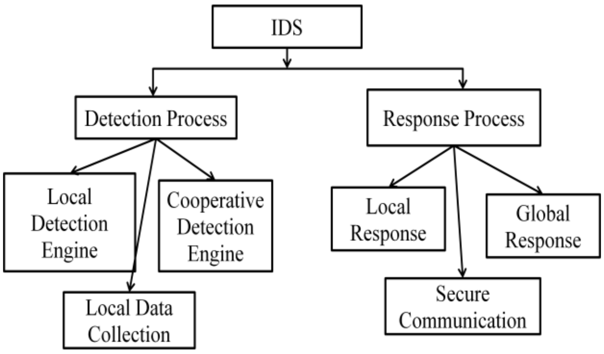

Fig 2: Basic Structure of IDS

Based on the MANET infrastructures, the movable ad hoc network can be configured to either flat or multi-layer. Based on the IDS structure see Figure 2, The MANET is classified into the following four types.

1) Standalone architecture.

2) Distributed and collaborative architecture.

3) Hierarchical architecture.

4) Mobile agent for IDS architecture.

3.3 IDS Basic Functions

To identify three main modules [13] in IDS: First, Monitoring Module for controlling the collection of data. Next, Analyses Module for deciding if the collected data indicated as an intrusion or not. Finale, Response Module for manage and using the response actions to the intrusion

3.4 IDS Classification

Intrusion detection is an essential in any high survivability MANET network. The main obstacle is to construct intrusion detection and response solutions while preserving the desired network performance are basically following these types of models employed in current IDS.

Based on data collection mechanisms, The IDS can be classified as network based or host-based according to the audit data that is followed as

1) Network based (Independent Platform)

This IDS system is placed at a strategic point within the network to monitor traffic to and from all devices on the network.

2) Host based

This IDS system runs on individual hosts or devices on the network. It gives alert signal to user or administrator if any suspicious activity happened.

3) Stack-based (evolution to the HIDS systems)

4) Distributed IDS

Gather audit data and Detect attacks from multiple hosts and possibly the network that connects the hosts.

3.5 IDS Techniques for MANET

For Based on detection techniques, there are few main categories of IDS operation based on detection techniques for alarm triggering mechanism to be used as:

1) Signature-based (Misuse detection model)

Signature-based IDS generate an alarm, if fingerprint or signatures patterns are matched and it also maintains a signatures pattern of known attacks.

Drawback: Difficulty to gather signatures/ detect unknown attack and keep them up to date.

2) Anomaly-based detection (profile based detection)

Ability to rectifying previously unknown and insider attacks, without need for signatures.

Drawback: Generate large number of false positives alarm rate due to legitimate activity.

3) Specification-based detection

It's first defines a set of constraints which describe the correct operation of a protocol. After, it monitors the execution of the protocol with respect to the defined constraints.

3.6 Intrusion Detection and Prevention Systems (IDPS)

Primarily aware of IDPS [9] to isolate as possible logging information and produce reporting to security administrators and attempts to stop them. In additionally use, IDPSes for other reason, such as identifying problems with documenting existing threats, security policies, and deterring individuals from violating security policies. An intrusion detection and prevention system (IDPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. IDS can be categorize as Network based which does packet analysis on the boundaries of a network and Host based which identifies intrusion on host machine.

4. EVALUATION METRICS FOR MANET ROUTING PROTOCOLS

As numerous applications have different services, requirements required by them and the associated QoS parameters differ from application to application.

4.1 Routing Protocols for MANET

An Mobile Ad-hoc routing protocol is a convention or standard that controls how nodes come to agree which way to route packets between computing devices in a MANET. A primary goal of routing protocol [15] is used to discover routes establishment between nodes for exchanging messages may be delivered in a timely manner. Route creation should be done with a minimum of overhead and bandwidth consumption. In routing ad-hoc networks, nodes do not have a priori knowledge of topology of network around them. Since, the basic idea is that a new node discovers its presence and listens to broadcast announcements from its neighbor's mobile node. The mobile node learns about new near nodes and ways to reach and announces them, that it can also reach those nodes. After as the time on, each node knows about all other nodes and one or more ways how to reach them.

Routing algorithms must have to, Keep routing table relatively less. Pick best route for given destination. Keep table up-to-date when nodes die or move. Require small amount of messages/time to converge.

4.2 Categorization of Ad-Hoc Routing Protocol

Each routing protocols are quite distinct, may generally be categorized as: (1) Table-Driven and (2) Source Initiated On-Demand Driven. The Solid lines as see Figure 3 represent direct descendants while dotted lines depict logical descendants.

a) Proactive Routing Protocols (Table driven)

- ➢ All times Maintain routing information on all nodes in the network which can be achieved by event driven routing information distribution and regular distribution of updated routing information.

Feature: Setup lower route latency.

Drawbacks: High routing overhead (periodic distribution of routing information).Stale routing information is highly dynamic topologies.

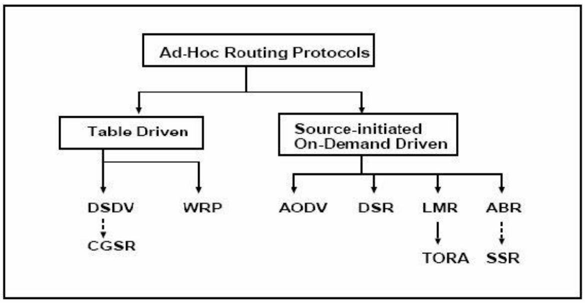

Fig 3: Routing Protocol Categorization

b) Reactive Routing Protocols (On Demand)

- ➢ Preserve routing information for each node which are needed and only for the time when they are needed.

Drawbacks: Set up larger route latency. Discovery route packet flooding.

c) Hybrid Routing Protocols (Other Routing Protocol)

- ➢ The hybrid routing is proactive for short distances and reactive for long distances. EX: Zone Routing Protocol.

Merits: Cut down the impact of proactive and reactive routing protocols. No setup route latency due to short distance connections.

5. RESEARCHES ACHIEVEMENT IN COMPARAE & EVALUTE VARIOUS IDS METHOD FOR MANET

Since traditional wired systems are not well suited to Ad hoc network in IDS, because many researchers have proposed several distributed IDS especially for ad hoc network, out of which some of them will be reviewed in this section.

5.1 Preventing of DOS Attacks using AIDP Mechanism

- Nadeem, A., [3] has proposed a preventing DOS attack using AIDP mechanism.

Process of Nadeem Proposed System

Assess control chart, a tool used in statistical process control (SPC) for detecting DOS [20] which produces low detection & high false alarm rates. To overcome above mentioned problem they used adaptive intrusion detection & prevention (AIDP) mechanism. Finally, they isolated and prevent the intruder nodes from the network.

Two stage process:

- ➢ Initially use chi-square test as an ABID mechanism to initially check the overall behavior of the network.
- ➢ Next uses control chart to identify intruding nodes.

Drawbacks: Absence of Misused Based Intrusion Detection (MBID).AIDP is more prone to generate false positives than MBID and also an affordable processing overhead on the network.

5.2 Based on Acknowledgement to Provide Security in EAACK Model

- Elhadi M. Shakshuki & Nan Kang [12] to improve the technology and reduce the hardware costs, they implemented a new intrusion detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANET network as see Figure 4. Compared to current approaches, EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances.

Process of EAACK Proposed System

Packet-dropping attack is always a major threat to the security in MANETs to avoid this paper proposes and implements a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) specially designed for MANETs and compared against it other popular mechanisms such as Watchdog, TWOACK, and AACK in different scenarios through simulations.

EAACK greatly demonstrates higher malicious behavior detection rates in certain circumstances while does not affect the network performances.

In this proposed EAACK scheme implemented both DSA and RSA, which is consisted of three major parts, namely, ACK, Secure ACK (S-ACK), and Misbehavior Report Authentication (MRA).

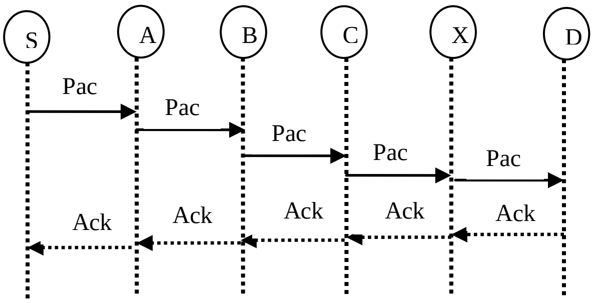

Fig 4: EAACK Control Flow Diagram

EAACK is an acknowledgment-based IDS to prevent the attacker from forging acknowledgment packets during the packet transmission process, so avoid this they incorporated digital signature in his proposed scheme. To ensure in order of integrity of the EAACK, IDS requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted.

Problems Identification

Watchdog system fails to detect malicious misbehaviors node. TWOACK acknowledgment process required in every packet redundant transmission process can easily degrade the limited battery power. Still AACK suffer from the problem that they fail to detect malicious nodes [19] with the presence of false misbehavior report and forged acknowledgment packets.

Problems Definition of EAACK model

In this research work paper, EAACK have resolved the problem of Watchdog, TWOACK & AACK model and which also solves not only receiver collision and limited broadcast power but also the reduce misbehavior problem [18].

Advantages: Demonstrated positive performances, limited transmission power and reduced receiver collision.

Drawbacks: DSA scheme consumes more battery power and computational power.

5.3 IDS Method for Distributed & Cooperative Architecture

- Farhan Abdel-Fattah [8] has presented a distributed and cooperative architecture for statistical anomaly detection where individual IDS agent are placed on each node which monitors user activities, system activities and communication activities within radio limited range; notice to identify intrusion and initiates a response.

Process of Farhan Proposed System

The proposed model implement distributed and cooperative architecture in nonoverlapping region framework through makes use of machine learning techniques in order to achieve efficient and effective intrusion detection. This model combines the flexibility of Anomaly detection mechanism used with the accuracy of a signature-based detection method.

They expose two anomaly methods for improving the IDS approach for detecting detailed information of attack types and sources.

a) Conformal Predictor K-Nearest Neighbor (CP-KNN).

b) Distance-based Outlier Detection (DOD).

Detected attacks classified into two types:

➢ Strong and Weak attack. Based on attack assign local alarm goes generated into three levels of processing which is the inside node, region and global node for each attacks. This proposed design of IDS model consists of two major components following as see Figure 5:

1) Gateway Intrusion Detection (GID)

2) Local Intrusion Detection (LID)

GID node can optimize energy apply by scheduling only a subset of region members who will activate their monitoring sensors agents at one time. Other region members can minimize their energy consumption at the same time.

GID divided into 3-modules such as Global Detection Model (GDM), Global Response Module (GRM) & Cooperation Module (CM).

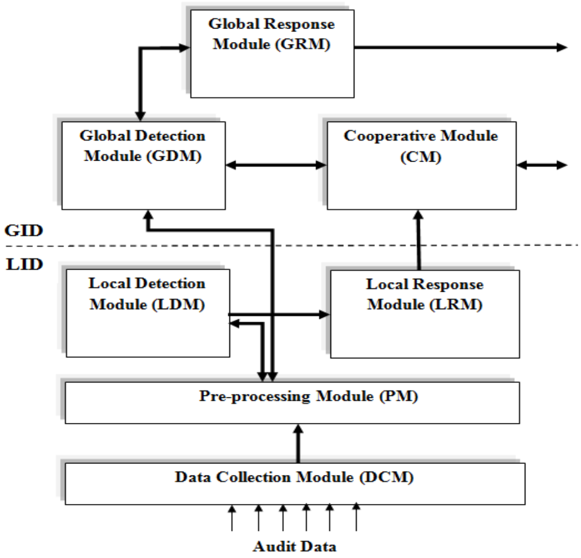
Global Response Module (GRM)
Global Detection Module (GDM)
Cooperative Module (CM)
GID
LID
Local Detection Module (LDM)
Local Response Module (LRM)
Pre-processing Module (PM)
Data Collection Module (DCM)
Audit Data

Fig 5: Intrusion Detection Architecture Design

Local Intrusion Detection (LID) contains different modules such as DCM, PM, LDM and LRM.

In initial process of Data Collection module (DCM) is various ad hoc networks to collects audits data sources and pass it to the PM. Next, Pre-process Module (PM) selects informative feature from all set of features, then pass these features to the LDM. After that, Local Detection Module (LDM) analyzes and collects the local data using CP-KNN and DOD classification algorithms for isolate malicious nodes in the ad hoc network. Finally, Local Response Module (LRM) to provided analyzed report to cooperation module.

This model implements a detection algorithm for testing the detection approach over three common attacks dataset [16] (resource consumption attack, dropping routing traffic Attack and black hole attack).

Merits: To achieve low false positive rate, high detection accuracy rate.

5.4 Compare & Evaluate Distinct IDS Architectures

- Christos Xenakis [2] have compared various IDS architectures for MANETs classified as:

(i) Stand-Alone Architectures

- Used as intrusion detection engine installed at each node consume only the node’s local audit data.

- Due to the distributed nature of MANET mobility, The solutions of local audit data only to resolve malicious behaviors within limits in terms of detecting the detection accuracy and the type of attacks.

(ii) Cooperative Architectures

- Similarly to stand-alone which also include an intrusion detection engine installed in every node but it can monitors and exchanges local audit data.

- Detection outcomes compare with neighboring nodes in order to resolve uncertain/ inconclusive detections.

(iii) Hierarchical Architectures

- Its multilayer approach by dividing the network into clusters. Specific nodes are selected to act as cluster-heads.

- Naturally simple cluster members run a lightweight local intrusion detection engine that performs discovery only on local audit data, while the cluster-heads run as a second layer of detection based on audit data from all the cluster members that acts a more comprehensive engine that.

5.5 Evaluation of classification algorithms for intrusion detection in MANET

- Sergio Pastrana, Aikaterini Mitrokotsa [6] monitoring proliferation of these MANET networks and their use in critical scenarios (like battlefield communications or vehicular networks) require new security mechanisms and policies to guarantee the authenticity, security and availability of the transmitted data. Effective comparison of six different classifiers to detect malicious activities in MANET. Genetic Programming and Support Vector Machines may help considerably in detecting malicious activities in MANETs.

Process of Sergio Pastrana Proposed System

- Discriminate ‘‘normal’’ against “intrusive’’ behavior effectively.
- Six well-known classification algorithms compared with several hyper-parameters have performed to various traffic conditions.
- Detection of four types of different attacks: Black Hole, Forging, Packet Dropping and Flooding have been focused.
- Concluded Genetic Programming may be a good paradigm to use when the goal is just to detect an intruder, then it is better to use a SVM classifier.

Drawbacks

When compare to other classifier (MLP, the Linear and Naïve Bayes classifier), they decided GP algorithm as good multiclass classifier. But it has highest detection rate only is Flooding attack.

5.6 Protecting the Range of Attacks using a GIDP Mechanism

- Adnan Nadeem & Michael Howarth [10] has adopted Generalized Intrusion Detection and Prevention (GIDP) mechanism for protecting various unknown attack. Detection and prevention of a specific kind of attack such as sleep deprivation, black hole, grey hole, and rushing or Sybil attacks on MANET has been focused. GIDP mechanism uses the combination of anomaly-based and knowledge based intrusion detection to secure MANETs from a wide variety of attacks. The impact on the MANET performance of the various attacks and the type of intrusion response has been investigated.

Process of Adnan Proposed System

In his existing they use AIDP mechanism for preventing known DOS attack only. Avoid this problem; Adhan [10] has introduced Generalized Intrusion Detection & Prevention (GIDP) mechanism as see Figure 6.

GIDP use a combination of anomaly-based and knowledge-based ID that can protect MANETs against a variety of attacks. So, it can also identify new unexpected or known attacks.

GIDP Architecture

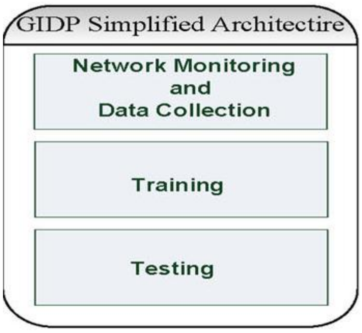
GIDP Simplified Architectire
Network Monitoring and Data Collection
Training
Testing

Fig 6: GIDP Architecture Process

- GIDP monitors the network and collects audit data specific for intrusion detection throughout the network’s lifespan.

- Once the network is established, Training is performed for N time intervals (TI) to obtain an initial training profile (ITP).
- The Testing module is then called after the training module has run, and this continuously tests the network for intrusion detection and prevention after each further TI.

Modules

It is possible to identify three main modules in IDS such as

(i) Data Collection modules for Collection of Audit data from the nodes.

(ii) Detection modules for deciding if the data collected indicated as intruder or not.

(iii) Response modules for if there is any intrusion, response module sends alert report to all the nodes.

Algorithm and Techniques

This paper employs cluster head (CH) in two phases:

1) **Training Phases**

CH continuously applies the GIDP training module for N time intervals (TI), resulting in initial training profiles (ITPs) of NCM and DM.

2) **Testing Phases operates GIDP in three stages.**

a) Intrusion Detection.

b) Identifying Attack and Inferences.

c) Identification and Isolation of Intruding Nodes.

Expected Outcomes

This model gives more effectively identifying attacks and sufficiently improves the network performances. Protect MANETs from a wide variety of new unforeseen attacks with an affordable network processing overhead. The proposed mechanism improves detection accuracy rate and reduces false positive alarm rate.

5.7 Secure Leader Election Model for Intrusion Detection in MANET

- In Vickrey, Clarke, and Groves (VCG) model [11] to ensure truth-telling to be the dominant strategy for any node using reputation system model as see Figure 7.

Problem Identification

To balance the resource consumption among all nodes in the prolong lifetime of an MANET nodes with the most other remaining resources should be elected as the leaders. Two main barriers in achieving this goal are.

1) Without incentives for serving others, a mobile node may behave selfishly by lying about its remaining resources and avoiding being elected.

2) Electing an optimal collection of leaders to minimize the overall resource consumption may acquire a prohibitive performance overhead.

Techniques Used

In this paper, they study leader election in the presence of selfish nodes for IDS in MANETs. To issue the address of selfish nodes, they present a solution provided to nodes based on mechanism design with in the form of incentives reputations to encourage nodes in honestly participating in the election process.

Based on amount of incentives, it's used the Vickrey, Clarke, and Groves (VCG) model which ensure truth-telling to be the dominant strategy for any node. In VCG model, Leaders are elected in a manner to ensure optimum resource utilization. Two schemes are proposed to issues the address:

a) Cluster-Dependent Leader Election (CDLE)

b) Cluster-Independent Leader Election (CILE)

Detection of Suspected Node

To address the optimal election issue, they propose a series of local election algorithms that can lead to globally optimal election results with a low cost.

To address the selfish behavior, incentives are designed in the form of reputation to encourage nodes to honestly participate in the election scheme. Reputation System Model is used to

1) Motivated nodes to act normally

2) Punish the misbehaving nodes.

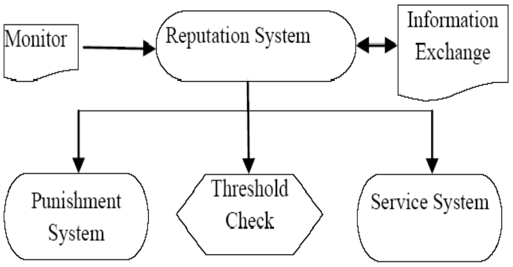

Fig 7: Reputation system model

Advantage

To decrease the percentage of single-node cluster head leader and maximize cluster size. Allow the properties for improving the detection service through distributing the sampling budget over less number of nodes and reduce single nodes to launch their IDS.

5.8 Detection of Selfish Node using IDS for MANET

- Charlie Obimbo & Liliana Maria Arboleda-Cobo [7] has proposed system of enhancement of the Watchdog / Pathrater form of Intrusion Detection in MANET.

IDS Techniques for Manet

Selfishness may exhibit one of the different kinds of misbehaviors' a node. A selfish node to preserve its own resources while using the other services and consuming their resources.

Detection of Selfish Node

The Watchdog/Pathrater has produced a solution to the problem of selfish (or "misbehaving") nodes in MANET. Two extensions of DSR algorithm to mitigate the effects of routing misbehavior in selfish nodes are.

a) Watchdog → Detect the misbehaving nodes.

b) Pathrater → Respond to the intrusion by isolating the selfish node from the network operation.

Process of Charlie Proposed System

They implement a schema similar to Watchdog and Pathrater on top of DSR.

The basic characteristics of this implementation are the use of additional information in the routing messages and some unnoticeable variations to the control of forwarded messages.

They modify the DSR Agent directly, which is the easiest way to complete the task in such a limited time.

Role of Watchdog / Pathrater

- **Watchdog Module**

- Watchdog runs on each node when forwards a packet that verifies next node in the path.

- If the next node cannot forward the packet, then it is considered to be misbehaving and is reported by sending an alarm message to the other nodes on its friends list.

- The Watchdog module was implemented by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match.

- **Pathrater Module**

- After the Watchdog module detects the malicious node, the Pathrater module then deletes the corresponding route from the route cache and tries to determine if there is another route available to the destination.

5.9 IDS for Mobile Agent in a Non-Overlapping Zone Approach

- Farhan A.F., Zulkhairi D., M.T. Hatim [14] proposed an intrusion detection system for ad hoc networks based on mobile agents, wherever selected nodes are facilitated with sensors to collect and merge audit data implementing a cooperative detection algorithm which reduces resource consumption.

Process of Hatim Proposed System

- Using lightweight mobile agent can be achieved by Data Collection & Analysis in non overlapping zone framework.

- Detected events into two types, strong and weak events in new hierarchical distributed IDS for MANET.

- Weak event goes into different levels of processing; this is the node level, zone level and network level.

Merits:

- To alert the Alarm message by reduce the data transmission to save the bandwidth resource in the MANET.

6. SUMMARIES OF REVIEWED IDS FOR DETECTING MISBEHAVING NODES

This section gives a summary of the intrusion detection methods for Mobile ad hoc networks with different parameters using various IDS engine for a range of methodologies to detect the abnormal behaviors. The IDS is measured by varying mobility of nodes, traffic and various characteristics of a network. Collected audit data for detection may be from single, multiple and cross layer. Most part of the IDS collected data from network layer and some of the IDS used the cross layer data. Mobile Ad-Hoc routing protocols categorized into table driven and on demand. The entire IDS considered the On Demand Routing protocols. By attacks on MANET mainly target the network, transport and MAC layer since these layers perform the critical functionality. The performance of Reviewed IDS handle only a limited set of attacks pertains to single layer.

7. CONCLUSION AND FUTURE RESEARCH WORK

This paper analyzing the various methods & architectures of IDS technique for MANET we come to a conclusion that IDS architecture that involves cross layer design using autonomous mobile agent based architecture which is distributed and cooperative can efficiently detect the abnormalities and is more suitable for MANET. Apart from architectural issues, data gathering techniques like trust or reputation based, monitoring based and feedback based determines the false positive rates. Among existing anomaly detection systems, distributed intrusion detection algorithms are more economic due to distributed nature of ad hoc network. Intrusion prevention techniques alone are not enough to secure ad hoc network. Because of, security is the most important feature for deployment in mobile Adhoc network. Hence requires a more efficient intrusion detection system.

The future breadth of work also includes combining trust based, monitoring based and probing based techniques in various attack scenarios to develop intrusion detection techniques using mobile agents which will reduce the false positives and improve detection and prevention effectiveness.

Acknowledgments

I am indebted to my (PhD) guide Mrs.A.Annalakshmi for giving me an insight on intrusion detection systems.

8. REFERENCES

[1] Ali Ghaffari**. "Vulnerability and Security of Mobile Ad hoc Networks"**. Proceedings of the 6th WSEAS International Conference on Simulation, Modeling and Optimization, Lisbon, Portugal, September 22-24, 2006.

[2] Christos Xenakis., Christoforos Panos., Ioannis Stavrakakis. **"A comparative evaluation of intrusion detection architectures for mobile ad hoc networks"**. ELSEVIER Computers & Security 30(2011), page no 6 3 – 80.

[3] Nadeem, A., & Howarth, M. (2009). **"Adaptive intrusion detection & prevention of denial of service attacks in MANETs"**. In Proceeding of ACM 5th international wireless communication and mobile computing conference. Germany, June16.

[4] Karan Singh, R. S. Yadav, Ranvijay, **"A REVIEW PAPER ON AD HOC NETWORK SECURITY"**. International Journal of Computer Science and Security, Volume (1):Issue (1)

[5] Levente Butty, Jean-Pierre Hubaux, **"Report on a Working Session on Security in Wireless Ad Hoc Networks"**. Mobile Computing and Communications Review, Volume 6, Number 4.

[6] Sergio Pastrana., Aikaterini Mitrokotsa., Agustin Orfila., Pedro Peris-Lopez. **"Evaluation of classification algorithms for intrusion detection in MANETs"**.

ELSEVIER Knowledge-Based Systems 36 (2012) 217–225.

[7] Charlie Obimbo, Liliana Maria Arboleda-Cobo. **"An Intrusion Detection System for MANET"**. Communications in Information Science and Management Engineering (CISME) Vol.2 No.3 2012 PP.1-5 www.jcisme.org ○C 2011-2012 World Academic Publishing.

[8] Farhan Abdel-Fattah., Farhan Abdel-Fattah., Shaidah Jusoh. **"Distributed and Cooperative Hierarchical Intrusion Detection on MANETs"**. Published by International Journal of Computer Applications (0975 – 8887) Volume 12– No.5, December 2010.

[9] Pin Nie, **"Security in Ad hoc Network"**, 2006.

[10] Adnan Nadeem, Michael Howarth. **"Protection of MANETs from a range of attacks using an intrusion detection and prevention system"**. © Springer Science + Business Media, LLC 2011.

[11] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi, and Prabir Bhattacharya. **"Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET"**. In Proceeding of IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011.

[12] Elhadi M. Shakshuki., Nan Kang, Tarek R. Sheltami. **"EAACK—A Secure Intrusion-Detection System for MANETs"**.IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3 MARCH 2013 1089.

[13] Li, Z., Das, A., & Zhou, J. (2005). **"Theoretical basis for intrusion detection"**. In IEEE workshop proceedings on information assurance and security, 15–17 June (pp. 184–192).

[14] Farhan A.F., Zulkhairi D., M.T. Hatim. **"Mobile Agent Intrusion Detection System for Mobile Ad Hoc Networks: A Non-overlapping Zone Approach"**. ©at UNIVERSITI UTARA MALAYSIA from November 11, 2008 IEEE Xplore onwards.

[15] Sanzgiri, K., & Belding-Royer, M. (2002). **"A secure routing protocol for ad hoc networks"**. In Proceedings of 10th IEEE international conference on network protocol (ICNP' 02).

[16] Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007). **"Detecting black hole attack in tactical MANETs using topology graph"**. In Proceeding of 32nd IEEE conference on local computer networks.

[17] Zhang, Y., & Lee, W. (2000). **"Intrusion detection in wireless adhoc networks"**. In Proceeding of 6th ACM MOBICOM.

[18] Yu, W., & Ray, K. (2005). **"Defence against injecting traffic attack in cooperative ad hoc networks"**. In IEEE global telecommunication conference Globecom.

[19] Yi, P., Dai, Z., & Zhang, S. (2005). **"Resisting flooding attack in ad hoc networks"**. In Proceeding of IEEE conference on information technology: coding and computing, Vol. 2 (pp. 657–662).

[20] 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.

9. AUTHOR'S PROFILE

I am Arunkumar.R currently doing M.E (Computer Science & Engg.) from K.S.R College of Engineering and received B.E (Computer Science & Engg.) from Anna University in 2011. I was worked as Software Engineer in Igate Patni Technical Solution.

Mrs.A.Annalakshmi received B.E (Computer Science & Engg.) from M.S.University in 2003, M.E (Computer Science & Engg.) from Anna University in 2009. She has worked as Assistant Professor in Nandha Engineering College between 2004-2012. Currently she is working as Associate Professor in the Dept. of CSE, KSR College of Engineering, Tiruchengode, Tamil Nadu, India. She is a life member of ISTE. Her area of interest includes Computer Networks and Network Security.