International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Intrusion Detection Methods in MANET: A Survey

Prerna Priyadarshini * & Mrs Neeti Kashyap**

ITM University, Gurgaon

ABSTRACT:

MANETS an acronym for Mobile AD Hoc Network is one of the most recent emerging trends in research areas of computer science. Mobile refers to movement, AD Hoc means temporary and Network meaning collection of nodes interconnected with each other. MANETS are self-organized, have dynamic topology, lack centralized administration, havelimited energy and constrained bandwidth.Due to such features these nodes are highly vulnerable to attacks. Real life applications of MANET are in military operations, disaster relief operations, enterprise.Hence, a higher level of security is needed.To achieve security, Intrusion detection system came into picture.In this paper an attempt has been made to compare traditional intrusion detection techniques with modern approaches used for intrusion detection.

Keywords*: Mobile Ad-hoc Network, Fuzzy Logic, Black-Hole Attack, Intrusion Detection Techniques.*

INTRODUCTION:

Mobile AD-Hoc Network is a collection of wireless mobile nodes forming a temporary network which means a node in the network can either join the network or leave it according to its own comfort. They neither have a fixed infrastructure nor centralized authority. Nodes in this network can communicate directly if they are within the radio range.For nodes outside the radio range, multi-hop communication is used. The figure given below illustrates a MANET.

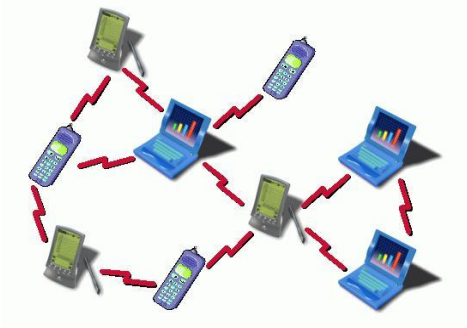

Fig. 1 MANET [http://www.ece.iupui.edu/~dskim/manet/images/adhocnet.gif]

Characteristics of MANETS

- **Dynamic Topology:-**Nodes in the network are free to join or leave according to their own comfort zone.
- **Multi-Hop Routing :-**For nodes outside the radio range, multi-hop routing is used for communication.
- **Limited Power Supply**:-Nodes in the network may behave in a selfish manner when it finds that there is only limited power supply.
- **No Predefined Boundary:-**MANET'S Topology is mainly affected by geographical location and radio range.Hence, it does not have a pre-defined boundary.
- **Distribution :-** MANET is distributed in its operation and functionalities such as routing ,host configuration and security.
- **Bandwidth Constraint:-** Low capacity link exists which are susceptible to noise, interference and signal attenuation effects.
- **Independent Nodes:-** Nodes in the network are independent and acts as both host and router.
- **No Infrastructure:-** No infrastructure is required to set up a network.

Applications of MANET

MANETS have numerous applications:

- **Military Operations: MANETS** can be used during military operations. Ad-Hoc networking can allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.
- **Virtual Classrooms and conferences:** MANETS can also be used for virtual classrooms and conferences. Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.
- **Simplification of inter communication through Bluetooth:**Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile A personal area network is a short

range, localized network where nodes are usually associated with a given person or phone etc.

- **Disaster Relief Operations**: MNAETS can also be used for relief operations. Ad hoc networks can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

Attacks in MANETS

MANETs due to their dynamic topology are highly vulnerable to various types of attacks. These can be categorized as under:-

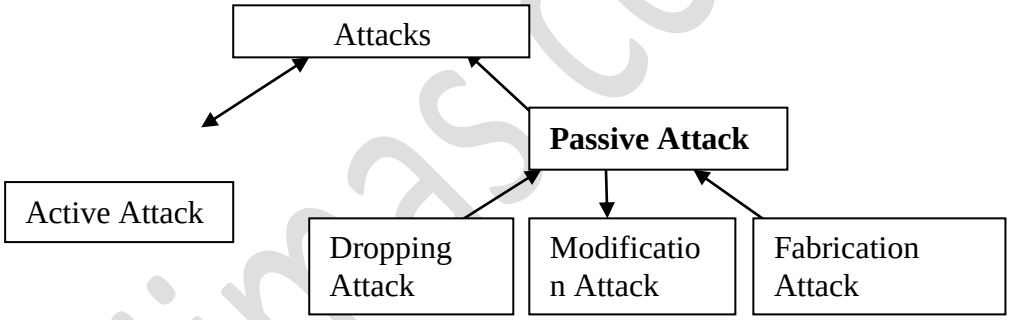

Figure 2.Attacks in Manets

- **Passive attacks**: A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.
- **Active attacks**: Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Active attacks are classified into four groups:

- **Dropping Attacks**: Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes.

Intrusion detection Techniques	Approach	Type of attack	Formula used	Algorithm used	Performance metric considered	Advantages	Dis advantages

- **Modification Attacks**:. These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.

- **Fabrication Attacks**: In fabrication attack, the attacker send fake message to the neighbouring nodes without receiving any related message.

Intrusion Detection System

It is defined as the tools, methods and resources to help identify, assess and report unauthorized network activity .Depending on detection techniques used, IDS can be classified into three categories.

DATA Detection Techniques

- **Signature or misused based**:- uses pre known attack scenarios and compare them with incoming packet traffic. Techniques such as expert system , pattern recognition are used.

- **Anomaly Based IDS**:- detect activities that differ from normal expected system behavior . Techniques such as statistics, neural network, data mining is used.

- **Specification based IDS**:- monitors the current behavior of the system according to specification that describe the desired functionality. A mismatch between the current behavior and specifications will be reported as an attack.

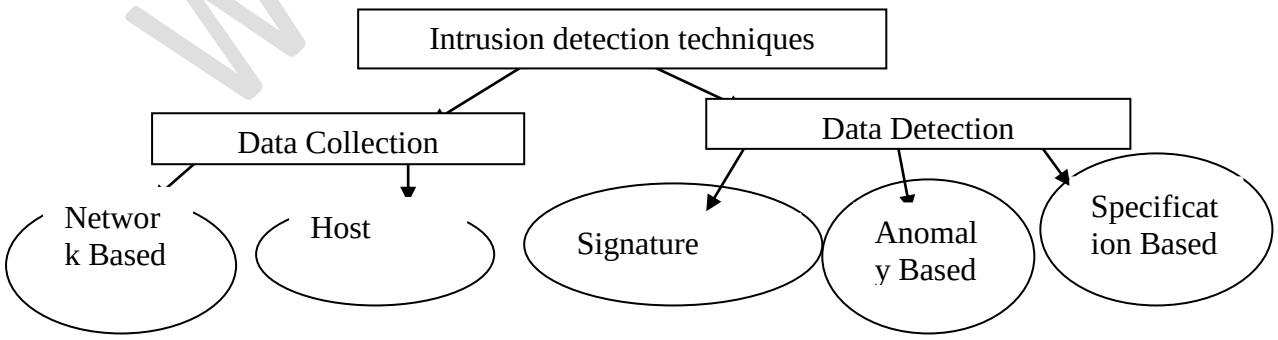

Figure-3 Intrusion Detection Techniques

Watchdog and Path rater (a survey on intrusion detection in mantes by Tiranuch Anantvalee, Jiewu)[]	Traditional approach	Packet Dropping Attack	Path metric= Node rating +link reliability	None	Path metric (by keeping rating of node)	Paths containing misbehaving nodes avoided	Misbehaving Nodes Encouraged To continue Their behaviour
CONFIDANT(a survey on intrusion detection in manets by Tiranuch Anantvalee, Jiewu)[]	Traditional approach	Packet Dropping	None	None	Level of trust	Misbehaving nodes not included in routing and stop them from forwarding packets	More opportunities for attackers to send false alarm
Leader Election Algorithm(Mechanism design based secure leader election by Noman Mohammed, Lingyu Wan)[]	Modern Approach	Fabrication attack	$Ci=\begin{cases} inf & \text{If } (Ei<Eid) \\ Psi - PF_i & \text{(otherwise)} \end{cases}$	Leader - election algorithm	Reputation System, payment, cost of analysis	Re-election is done to ensure that only a single node does not remain leader. (Malicious and selfish nodes are removed)	Proposed Algorithm has to be secure itself which is hard to achieve
Wormhole Attack (An efficient and secure Intrusion Detection Method in Mobile Adhoc Network	Modern	Packet Dropping All pass All Drops Threshold	Packet Delivery Ratio= Number of Packets recieved / Number of Packets Sent 2)Average end to end	None	1)Packet Delivery ratio 2)Average end-to-end delay 3)Through put 4)Jitter	Easy Computation	

using Intutionistic Fuzzy By-AnushaK, Jayaleshwari N, Rajya Lakshmi G V)[]			delay=time at first data packet arrived-time at first data packet sent)				
Black hole Attack (An efficient and secure intrusion detection method in mobile adhoc network using Intuitionist Fuzzy)[]	Modern Approach	Black hole Attack	Normalized Hamming Distance	AODV	1)Member-ship function 2)Non member-ship function	Computation is easy. Results are accurate	
Threshold Value Approach(An efficient and secure intrusion detection methods in mobile ad-hoc network using intuitionist fuzzy)[]	Modern Approach	Packet Dropping	Packet drop>threshold value	None	1)node number 2)Packets forwarded 3)Packets received 4)Threshold value	Easy computation	Not accurate
Gray Hole attack towards source and destination(An efficient	Modern approach	Dropping Attack	Membership function= Threshold-number of packets dropped	AODV	1)occurrence indication 2) Non occurrence indication 3)Assurabil	Calculation gets reduced. Easy Approach	None

and secure intrusion detection methods in mobile ad-hoc network using intutionistic fuzzy)[]			**threshold**		**ity indication 4)Non indicator indication)**		

Comparative Study of various Intrusion Detection Techniques

CONCLUSION

This review paperfocuses on various Intrusion Detection techniques available and makes a comparative study between them. We conclude that modern techniques are more beneficial compared to traditional ones. Modern techniques are embedded with features with the help of which we can overcome the drawbacks of the traditional approach.

REFERENCES

i. Anusha K, Jayaleshwari N, Arun Kumar, Rajyalakshmi G V "An efficient and secure Intrusion Detection Method in Mobile Adhoc Network Using Intuitionist Fuzzy" *International Journal of Engineering and Technology* (IJET) Vol 5 ISSN:0975-4024.

ii. Tai Hoon Kim, and S. Madhavi, "An Intrusion Detection system in Mobile Ad-hoc Networks" *International Journal of Security and its Applications*, Volume 2, July 2008.

iii. Sevil Şen, John A. Clark, "Intrusion Detection in Mobile Adhoc Network".

iv. Zhang Y, Lee W (2003) Intrusion Detection Techniques for Mobile Wireless Networks. Wirel Netw : 545-556.

v. ArunKumar, Abhishek M.K,Tejashwini. A.I, Niranjan J.T, Pradeep R.P "A Review on Intrusion Detection Systems in MANET" International Journal of Engineering Science and Innovative Technology (IJESIT) Vol 2, March 2013.

vi. Anusha K, ayaleshwari. N," Evaluation of Intrusion Detection Techniques in Mobile AD-Hoc Networks" *Journal of Theoretical and Applied Information Technology*, Vol 53.

vii. Tapan P. Gondaliya, Mahinder Singh " Intrusion Detection System for attack prevention in Mobile Ad-hoc Network" *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 3,April 2013.

viii. Tiranuch Anantvalee, Jie Wu "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" .

ix. Noman Mohammed, Hadi Ortok, Lingyu Wang, Mourad Debbai and Prabir Bhattacharya, "Mechanism design-based Secure Leader Election Model for Intrusion Detection in MANET".

x. Sonal, Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" *International Journal of Science and Research*(IJSR) Volume 2,August 2013.