Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Intrusion Detection Methods in MANET

Poonam J. Desai[1], Hiren J. Gondaliya[2]

[1]Computer Science & Engineering, SLTIET
[2]Computer Science & Engineering, SLTIET

Abstract *— Instruction detection in Mobile Ad Hoc Networks* is a hard work because these networks with motion change their topologies; exist without strong amount points where grouped traffic can be got broken up (into simpler parts); put to use base structure less protocols that are readily moved to taking care of expertly; and get support from on noisy, stopping at times radio making connections. needing payment to base structure less network safe news and supporting the power to make connections in the existence of persons fighting against one is chief Issue; as an outcome of that, make out the attack types and selecting a good at producing an effect go into discovery methods are especially important for Manet applications. The purpose of this paper is to guidelines on selecting go into discovery methods in MANET. To clearly make, be moving in the go into discovery methods in ad-hoc networks, We attempt to present a move near, with which some having existence go into discovery techniques can be got mixed together and more increased go into discovery techniques can be undergone growth that can be took up to radio ad-hoc networks.

Keywords- Mobile Ad hoc network; Security; Intrusion detection; Reputation system; Link strength; Malicious node; IDS

I. INTRODUCTION

Mobile ad-hoc network is formed by the getting together of some readily moved network points(nodes) which can act both as a sender as well as receiver for data communication. They are distributed networks which are self-organizing and self-maintaining. There is no fixed base structure in the network, the topology changes with motion.[1] As an outcome of as an unbroken stretch changing topology, there is no fixed division line of the network. The network points be working together with each other to forward the facts packet. In such a network where there is no well-outlined division line, open medium, node get support from on one other to forward the facts packet, firewalls can not be send in name for getting these networks. go into discovery system is used in these networks to discover the without shame in the network. go into discovery system act as a second level in MANET ad-hoc networks.

In Present years, the safety issues are most important concerns in mobile ad hoc network. In comparison to wired network the mobile ad hoc network is more made open to being attacked. Because of its fundamental Properties, such as dynamic topology, limited power and limited bandwidth, it is very hard to achieve complete security in the mobile ad hoc network. Attack prevention method like encryption and authentication are not enough for reducing the possibilities of attacks. However, these methods are designed to prevent for a group of possible known attacks. These methods are not able to prevent newer attacks that are originated in the existing security measures. For this reason, a second mechanism is needed to detect and response for these newer attacks. The objective of this paper is to explore and to classify current techniques of Intrusion Detection System (IDS) aware MANET. In this paper we have study various intrusion detection techniques in MANET and then the comparison among several makes observations good things done will be valued based on their parameters.

II. SYSTEM ARCHITECTURE

The main task of the intrusion detection system (IDS) is to discover the intrusion from the network packet data or system audit data. One of the major problems that the IDS might face is that the packet data or system audit data could be overwhelming. Some of the features of audit data may be redundant or contribute little to the detection process. Some of the features of looking over of accounts by expert facts may be redundant or send in (writing) little to the discovery process. So the copies of smaller size in the size of facts(data) put is needed. To perform the reduction, two methods of feature selection, namely, markov blanket discovery and genetic algorithm are proposed.

The Intrusion Detection System is distributed in nature so each node of a mobile ad hoc network equipped with an IDS. System architecture of IDS comprises four components:

- Data collection module
- Profile module
- Feature selection module
- Intrusion Detection and Response Module

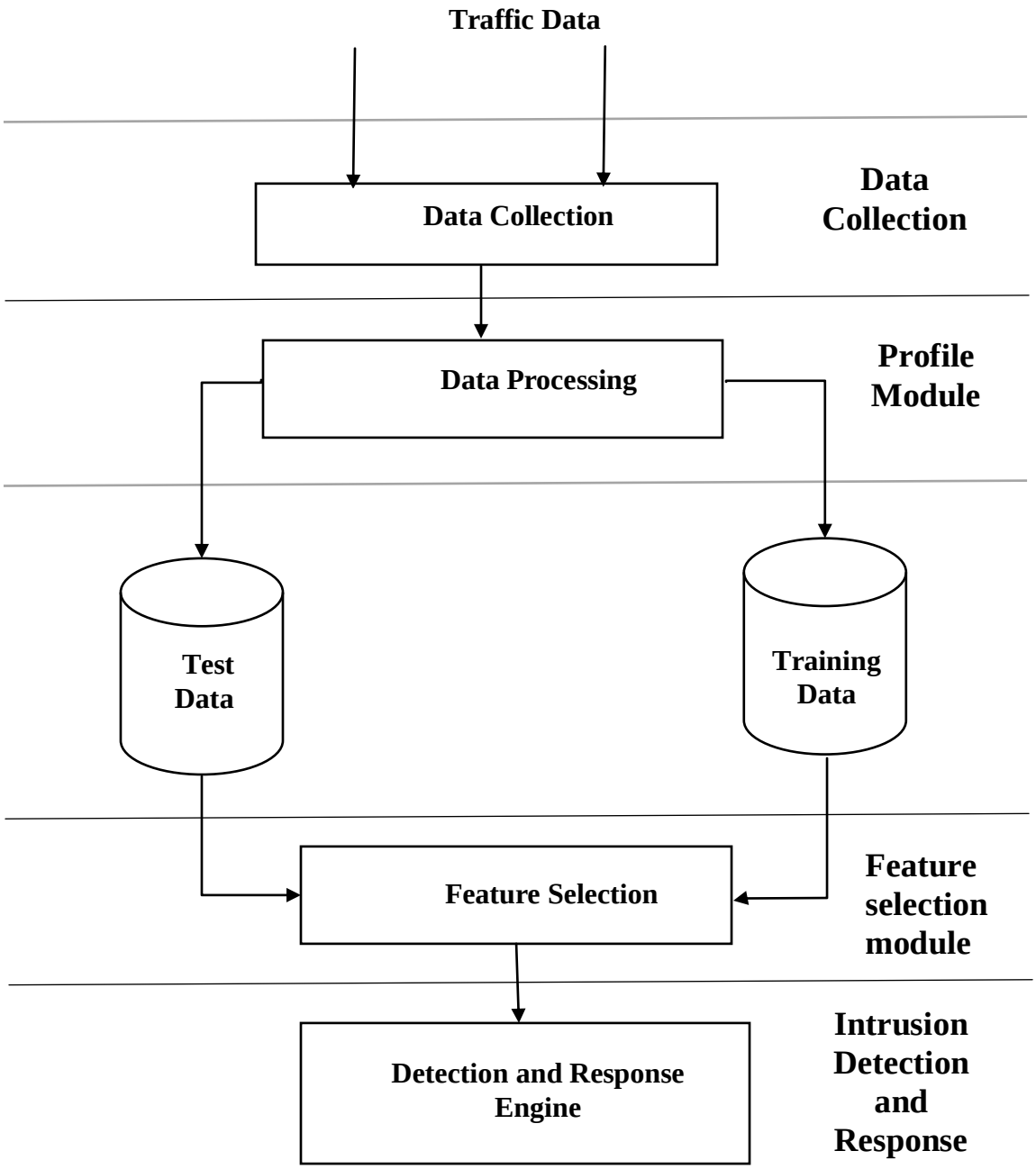

Figure 1. Proposed intrusion detection model

A. Data collection module

The part of a greater unit collects looking over of accounts by expert facts for each network point. The offered system gives thought to as unknown attacks. So the IDS need normal behavior of the system (normal outline) and breaking of normal behavior (attack outline). Normal outline is made come into existence using the facts self-control during the normal scenario. Attack outline is made come into existence by acting the part of the attacks.

B. Profile module

In this part of a greater unit looking over of accounts by expert facts is greatly changed into right form and size for the discovery process. From the attack facts, training facts put is made come into existence to train the bayesian classifier. Training facts is chiefly of making tickets giving name of events whether it is a normal event or an attack. Test facts is self-control under acted the part of attack general condition and it is given to the bayesian classifier to make out an event whether it is an attack or normal..

C. Feature selection module

Point selection is the process of selecting important features from the greatly sized facts put. The selected features are on the point to the discovery process. In order to act this operation the supporters point selection careful way is offered. Random population bayesian constructor rightness computation.

- Random population
- Bayesian constructor
- Fitness computation

D. Intrusion Detection and Response module

This part of a greater unit makes discovery of amount gone away from straight from the normal, general. In order to discover the seeming errors bayesian classifier is used. Classifier will be trained by the training facts. The test facts will be given as input to the trained bayesian classifier. Any amount gone away from straight from the edge level is taken into account level as seeming errors. Once all the attacks are taken to be then the letter making note will be given to all the network points in the ad hoc general condition.

III. *ATTACKS IN MANET*

The MANET is easily effected to passive and active attacks. The Passive attacks representatively have to do with only hearing private talk on purpose of facts, in view of the fact that the active attacks have to do with actions did by persons fighting against one such as copying, adjustment and thing taken out of exchanged facts. In particular, attacks in MANET can cause congestion, give birth wrong design for the way information, put a stop to services from working rightly or shutdown them completely. network points that do the active attacks are thought out as to be bad, and has relation to as put at risk, while network points that just drop the packets, purpose of amount made less given of blows living are taken into account to be self-interested. A self-interested network point does not take part in the sending the way protocols and also not forwarding packets in the network. In addition, a put at risk network point may use the sending the way protocol to give advertisement itself as having the shortest footway to the network point whose packets it wants to put a stop to as in the so called black hole attack.

A. Security Attacks Classification

Passive Attacks -Eavesdropping, traffic analysis, monitoring
Active Attacks- Jamming, spoofing, modification, replaying, DoS

B. Security Attacks on Protocol Stacks

Application Layer- Repudiation, data corruption
Transport Layer- Session hijacking, SYN flooding
Network Layer- Warmhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data Link Layer- Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical Layer -Jamming, interceptions, eavesdropping
Multi-layer attacks- DoS, impersonation, replay, man-in-the-middle

C. Cryptography Primitive Attacks

Pseudorandom number attack- Nonce, timestamp, initialization vector (IV)
Digital signature attack- RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack- SHA-0, MD4, MD5, HAVAL-128, RIPEMD
Security handshake attacks- Diffie-Hellman key exchange protocol, Needham- Schroeder protocol

D. Simulated attacks

Flooding attack
Black hole attack

III. INTRUSION DETECTION METHODS IN MANET

A. Method-1 Intrusion Detection In Mobile Ad Hoc Networks Using GA Based Feature Selection:

In this method, the seeming error discovery careful way is send in name for things not fixed ad hoc networks to discover the thing being force into. This careful way uses the network level knowledge for computers to give account of qualities the behavior of readily moved network points. The looking over of accounts by expert facts is self-control from all the readily moved network points under different scenarios to put in order the events. The normal outline is made come into existence under the being away of attacks and the attack outline is made come into existence by acting the part of attacks such as black hole and flooding. After getting together the looking over of accounts by expert facts, it was converted into a right form for the discovery process. The size of the looking over of accounts by expert facts is made lower, less with the help of point selection way of doing. In order to act the point selection operation handed down from father, mother and so on algorithm is used. The selected features are used for discovery. During the discovery process, the attack outline is made a comparison with the normal outline. If there is any amount gone away from straight from the normal behavior then the event is made ticket giving name as an attack. at last the doing a play of handed down from father, mother and so on point selection is valued based on discovery rate and false danger sign rate. This careful way uses fiction story point selection careful way, therefore it will give Reasonable getting better in doing a play.

B. Method-2 Intrusion Detection In Mobile Ad Hoc Networks Using Selective Watchdog Technique:

This method is is a getting better over the watchdog technique. IN watchdog each network point as an unbroken stretch hears its next network point sending (power and so on) but in the offered having selection watchdog way of doing only when the given credit for would not be received ,then IDS would start. Moreover, in watchdog way of doing all network points old flat warship their persons living near but in offered having selection watchdog way of doing ,network of network points are separated into clusters and only network points in the mass, group which have value greater than edge old flat warship their persons living near. In this letters used for printing system the source waits for the place where one is going to send given credit for to it after every 10th packet. If source gets the given credit for, then there is no without shame in the network and process goes on as such. But if the place where one is going fails to say one has had the facts packets for a time stage in time, then IDS starts its workings. Black-hole attack drops all the packets coming to it. As an outcome network operation drop with strong effect. The offered design makes discovery of the go into in the existence of black-hole attack in the network and the results shows that it is better than watchdog way of doing in terms of time to discover the go into and number of promiscuous hearing.

C. Method-3 Intrusion Detection In Mobile Ad Hoc Networks Using Reputation System

Reputation system module assigns and maintains reputation of different nodes. Reputation of any node can change due to:

- Self-observation
- WARNING Message, issued by neighboring nodes
- Avoid List, appended to the RREQ/RREP header

All the three ways have connected Reputation weights with greatest point weightage to self-observation. The Reputation is changed knowledge after every Time Window and information is communicated with the help of keep from lists, thereby keeping out of much of network overhead. A network point may be ticketed as Normal, having feeling that something is wrong or bad depending on the Reputation value connected with it. A network point may give lower, less important position to its Reputation by giving lower, less important position to its doing a play or it may get positive option of value on normal behavior. After each timing window Reputation system gets operation record of next go away nearby living person from old flat warship with number of packets for which it does not get sea full of broken ice, called as lost or dropped packets. The number of lost packets is then made a comparison with the MaliciousDropThreshold and if it is less, then the Reputation manager gives positive operation option of value else not. unlike having existence systems RISM system does not have a xed MaliciousDropThreshold, instead we have introduced the idea of a quality common to a group of congestion Parameter:

Congestion Parameter =Current queue status / Total queue length (1)

with the assumption that next nodes is also in same congestion state as the node in contention, misbehavior drop threshold is dynamically decided after each timing window as

MaliciousDropThreshold = MaxPacketRate × CongestionParameter (2)

In order to amount with the attacks on an of a certain sort Reputation system, like those of Collusion of untruth-talking persons and false suggestion note, the system has an insurance agreement that network points can be sorted bad only by Self-observation. It helps in nullifying the effect of attacks of false suggestion notes and Collusion of untruth-talking

persons as the false suggestion notes they put out on top, can only drop Reputation of network points to a certain amount, which is termed as a doubtful edge. After which, the system one and only depends upon its self-observation. suggestion notes and keep from List are only working well above doubtful board forming floor of doorway. in this way, a network point is declared bad eventually through self-observation only. whenever any network point has a Reputation in that sort and the coming to a decision network point gets any new suggestion note or keep from list Appearance, the system acts a make quickly Test, a test designed one and only for checking right,truth of a network point against whom the coming to a decision hard growth constantly gets such information. In this test, the coming to a decision network point produces a fake facts packet and forwards it to the network point in question. If next network points forward this packet good, then system gives it a doing a play option of value and clears its account else the network point is declared as bad. This test can be did only on network points in solid or the nearest one part of town. If the network point in question is actually bad, then it is likely to drop the test packet and for this reason, old flat warship shall go to person in authority its operation to Reputation manager and right steps are taken; other, its packets are forwarded and its account cleared.

IV. CONCLUSION

Security is the Major about in the ad-hoc networks as network points can be easily made prisoner or put at risk. Things not fixed ad hoc networks have a number of signicant safety issues which cannot be got answer to alone by go into discovery systems. In this paper we have seriously was looking at the having existence systems and outlined their power and shortcomings. The end of the current make observations is to make ready a great-sized picture of the current state of the make observations on IDS in MANET, and make ready a guideline on how to select go into discovery methods for IDS in MANET. The go into discovery system that has been offered and instrumented in this paper is based on different ways of doing. The system can discover thing being force into and right behavior in the network accurately.

REFERENCES

[1] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in Wireless/Mobile Security. New York: Springer-Verlag, 2008

[2] Giovanni Vigna and Richard A. Kemmerer, “NetSTAT: A network-based intrusion detection system”, Journal of computer security,1999,pp.37-71.

[3] B. Sun, “Intrusion detection in mobile ad hoc networks,” Ph.D. dissertation, Texas A&M Univ., College Station, TX, 2004.

[4] R. Nallusamy, K. Jayarajan, Dr. K. Duraiswamy “Intrusion Detection In Mobile Ad Hoc Networks Using GA Based Feature Selection”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2009, No.5(22), 25th December 2008.

[5] Animesh Kr Trivedi, Rishi Kapoor, Rajan Arora, Sudip Sanyal and Sugata Sanyal, ” RISM - Reputation Based Intrusion Detection System for Mobile Adhoc Networks”, Institute of Radio Physics and Electronics, University of Calcutta, December 18-20, 2006.

[6] Deepika Dua and Atul Mishra , “Intrusion Detection in Mobile Ad-hoc Network, “ in International Journal of Advanced Research in Computer and Communication Engg. ,vol.2,no.2,pp.5691-5694.

[7] Sonja Buchegger and Jean-Yves Le Boudec, “Self-Policing Mobile Ad- Hoc Networks by Reputation Systems” IEEE Communication Magazine, vol. 43, num. 7, p. 101(2005).