Particle Swarm Optimization Based Intrusion Detection for Mobile Ad-hoc Networks

MR. BHUSHAN S. CHAUDHARI
Research Scholar, Department of Computer Engineering,
Matoshri College of Engineering and Research Centre, Eklahare, Nashik, India
chaudharibs@gmail.com

DR. RAJESH S. PRASAD
Professor and Head, Department of Computer Engineering,
NBN Sinhgad School of Engineering, Ambegaon(Bk), Pune, India
rajesh.prasad@sinhgad.edu

Abstract:
In recent years, intrusion detection in mobile ad hoc network has become a topic of research. Due to problems like limited battery power, limited bandwidth and dynamic topology environment, it's very difficult to implement security measures for MANET. Routing protocols can play vital role in secure communication and intrusion detection. Particle swarm optimization is the bio-inspired approach based on swarm intelligence invented by James Kennedy and Russel Eberhart in 1995. A cooperative, distributed and low cost intrusion detection system can be built using PSO to prevent dynamic intrusive attacks in MANET.

Keywords: Mobile Ad-Hoc Network (MANET), Intrusion Detection Systems (IDS), Particle Swarm Optimization (PSO)

1. Introduction

A mobile ad hoc network is a self configuring network of computing devices without fixed infrastructure. Nodes in MANET are free to communicate and there is no provision of central authority as like server in wired networks. The fascinating characteristic of MANET is low cost of implementation. It has significantly been used in disaster management, military applications, virtual classrooms and conferences etc.

Any unauthorized access or non permitted attempt to access system or resource information is called intrusion. A device or software application that monitors network or system activities for malicious events is called intrusion detection system.

The starting section of this paper discusses about typical architecture and classification of intrusion detection systems for mobile ad hoc networks. Later part contains remarks about existing ID systems like Snort, OSSEC, OSSIM, Suricata, Bro, Fragrouter, BASE and Sguil and their limitations. Next section discusses about major attack types and challenges over MANET. Followed to which, detailed working of particle swarm optimization algorithm is explained. Paper concludes with proposed IDS solution using PSO and guidelines for future research.

2. Literature Survey

2.1 General Architecture of IDS

In general, an IDS is comprises sensors, analysis and configuration engine and a report system [12]. Sensors are responsible for gathering the appropriate data from the monitored system. Sensors may be internal to the system or external one.

An analysis and configuration engine is usually a centralized point that collects the data from the sensors and analyses them. This component might have to reconfigure the protected system accordingly if the results of the analysis indicate an intrusion during the response step. The response step might involve human interaction (e.g., the security administrator) or be fully automated. A report system is one that notifies the administrator for possible attacks.

In some IDS types (such as misuse detection IDS) a knowledge base which contains signatures of known attacks might also be present. This component is utilized by the analysis and

configuration engine during a step known as the data analysis step and it must be frequently updated to include the signatures of the latest attacks. Finally, it is possible for a response engine to exist. The response engine might be able to take actions automatically or after specific command of the administrator. Fig. 1 depicts a high level architecture of generic IDS that protects a network.

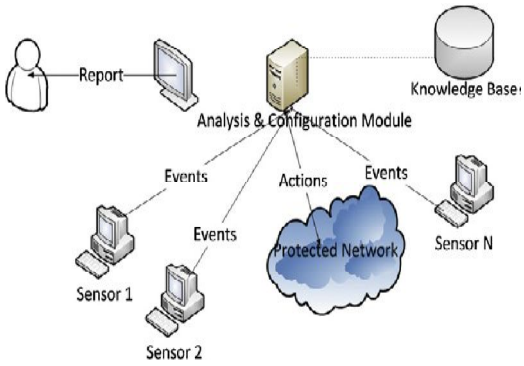

Figure 1: Architecture of typical IDS [12]

2.2 Classification of intrusion detection systems

IDS can be classified by number of different ways. Based on behavior after attack detection, it can be classified as active or passive IDS. Active intrusion detection system does not require operator intervention and can detect and prevent suspected attacks. It is also known as intrusion detection and prevention system (IDPS). Passive IDS is configured to analyze network traffic and alert operator for possible threats. It cannot take any corrective steps to secure network.

Further, based on the architecture type, IDS can be divided into Host IDS and Network IDS. A HIDS can only monitor nodes where agent software application is installed. It cannot monitor the entire network. Some of the well known HIDS products are Snort, Dragon Squire, Emerald eXpert-BSM, NFR HID, Intruder Alert etc. On the other hand, NIDS has separate management interface application for entire network. The network traffic is analyzed for suspects. Examples of network intrusion systems are: Cisco Secure IDS (formerly NetRanger), Hogwash, Dragon, E-Trust IDS [16].

Based on intrusion detection approach, IDS can be divided into signature based and anomaly based systems. Signature based IDS detect attacks with the help of evidences of previously known attack signatures. These footprints are called signatures are nothing but the footprints which intrusion leaves behind like number of failed login attempts, nature of data packets , file permissions accesses etc..

Anomaly-based Intrusion Detection Systems (IDS) learns from normal system activity patterns to identify new intrusion attempts. It is major challenge before researchers to design a low cost, robust anomaly detection system which can detect new attacks with minimum false alarm attack.

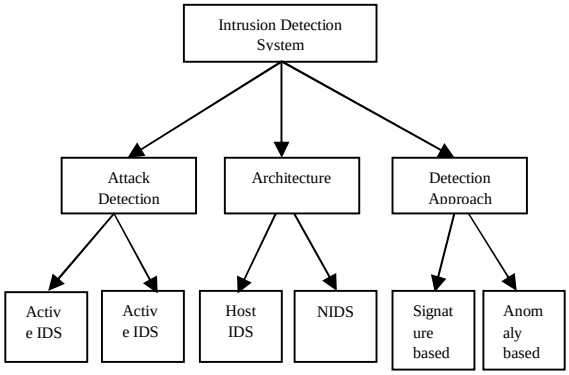

Figure 2: Classification of Intrusion Detection System

2.3 Existing Intrusions Detection Systems

- Snort: A free and open source network intrusion detection and prevention system was created by Martin Roesch in 1998 and now developed by Sourcefire. In 2009, Snort was declared as “greatest open source software of all time”. Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior using protocol used and content analysis.
- OSSEC: An open source host-based intrusion detection system, performs analysis of log records, periodic integrity checking, fatal rootkit detection, timestamps- based alerts and proactive response. OSSEC HIDS is widely used to monitor and analyze firewalls, web servers and authentication logs.
- OSSIM: The goal of Open Source Security Information Management, OSSIM provides a detailed analysis of network and all computational components to network administrator.

- Suricata: An open source-based intrusion detection system, was developed by the Open Information Security Foundation (OISF).
- Bro: An open-source, Unix-based network intrusion detection system. Bro detects intrusions in two steps. first parsing of network traffic to extract its application-level semantics is done and then event-oriented analyzers compare the activity with troublesome patterns.
- Fragroute/Fragrouter: A network intrusion detection evasion toolkit. Fragrouter helps an attacker launch IP-based attacks while avoiding detection. It is part of the NIDSbench suite of tools by Dug Song.
- BASE: The Basic Analysis and Security Engine, BASE is a PHP-based analysis engine to search and process a database of security events generated by various IDSs, firewalls and network monitoring tools.
- Sguil: Sguil is built by network security analysts for network security analysts. Its main component is an intuitive GUI that provides real-time events from Snort/barnyard. It also includes other components which facilitate the practice of network security monitoring and event driven analysis of IDS alerts.

2.4 Limitations of Existing IDSs

Most existing intrusion detection systems suffer from the following problems:

- First, the information used by the intrusion detection system is obtained from audit trails or from packets on a network. Data has to traverse a longer path from its origin to the IDS and in the process can potentially be destroyed or modified by an attacker.
  Furthermore, the intrusion detection system has to infer the behavior of the system from the data collected, which can result in misinterpretations or missed events. This is referred as the fidelity problem.
- Second, the intrusion detection system continuously uses additional resources in the system it is monitoring even when there are no intrusions occurring, because the components of the intrusion detection system have to be running all the time. This is the resource usage problem.
- Third, because the components of the intrusion detection system are implemented as separate programs, they are susceptible to tampering. An intruder can potentially disable or modify the programs running on a system, rendering the intrusion detection system useless or unreliable. This is the reliability problem[17].

2.5 Major Attack Types over MANET

Attacks in MANET can be classified in terms of consequence and techniques [19]. Based on consequence, attacks can be grouped into:

- Black hole: all packets are routed to a specific node which will not forward them at all
- Routing loops: cause a loop in routing path.
- Network partition: the network is divided into sub networks where nodes cannot communicate each other even though path exists between them.
- Selfishness: A node will not serve as a router for other nodes.
- Sleep deprivation: A node is forced to use up its battery.
- Denial of Service: A node is prohibited from sending or receiving packets.
- Cache poisoning: information in routing tables is modified, deleted or contains false information.
- Fabricated Route Messages: route messages, such as route requests and replies with malicious information are inserted into the network. They can be done by:
- False source route: a wrong route is broadcasted in the network, such as setting the route cost to 1 no matter where the destination is.
- Maximum sequence: alter the sequence field in control messages to the maximum possible value. This will cause nodes to invalidate all legitimate messages with reasonable sequence filed value.
- Rushing: In several routing protocols of MANET, only the messages that arrive first are accepted by the recipient. The attacker can block legitimate messages that arrive later by distributing a false control message.
- Wormhole: A path is created between two nodes that can be used to transmit packets secretly.
- Packet dropping: A node drops packets that are supposed to be routed.
- Spoofing: insert packet or control message with false or altered source address. Malicious

flooding: Forward unusually large amount of packets to some targeted nodes.

2.6 Challenges in Mobile Ad-Hoc Networks

In spite of availability of number of applications and prolonged improvement in mobile ad hoc networks, there are still certain issues and security challenges that we need to focus on [20]. Because of which MANET is still an elementary research field. Issues like dynamic nature of nodes, limited bandwidth availability and topology variations; none of security counter measures has yet claimed to be de facto standard. Some of the challenges in this field can be listed in following way:

- Unavailability of fixed channel makes it susceptible to outside signals.
- There is no fixed infrastructure in MANET. Hence, there isn't any central administrator for it. Every single node can communicate with any other node. Its bit difficult to manage faults in MANET due to dynamic topology environment.
- The medium of communication is unreliable.
- Network may suffer from Hidden terminal and exposed terminal phenomenon.
- As the network size may grow or shrink, node value in MANET may vary and it should be capable to handle overloaded communication with the same intensity.
- Most of the channel properties are time varying and are asymmetric.
- Each node has different transmission capability resulting in asymmetric links. Also there is no route present as interface among communicating nodes and may result in packet losses.

3. Particle Swarm Optimization (PSO)

Particle swarm optimization (PSO) is a heuristic optimization technique invented by Dr. Russel Eberhart and Dr. James Kennedy in 1995. This is nature inspired technique based on social behavior of birds flying in the sky in search of goal (food etc.) or fish behavior to get protection from giant fishes [1,10]. While flying, birds adjust their flying as per flying behavior of itself as well as other members of the flock. Each of the members tries to reach optimum position.

Each particle keeps track of best value achieved so far by it called *pbest* and the best value by neighboring coordinates called *gbest* as well. Particles keeps on changing their flying velocity (acceleration) based on pbest and gbest locations leading to optimum location. PSO has very few parameters to adjust and has proved to be an effective technique on routing challenges [4]. Each particle tries to modify its position using the following information:

- the current positions,
- the current directions,
- the distance between the current position and pbest,
- the distance between the current position and the gbest.

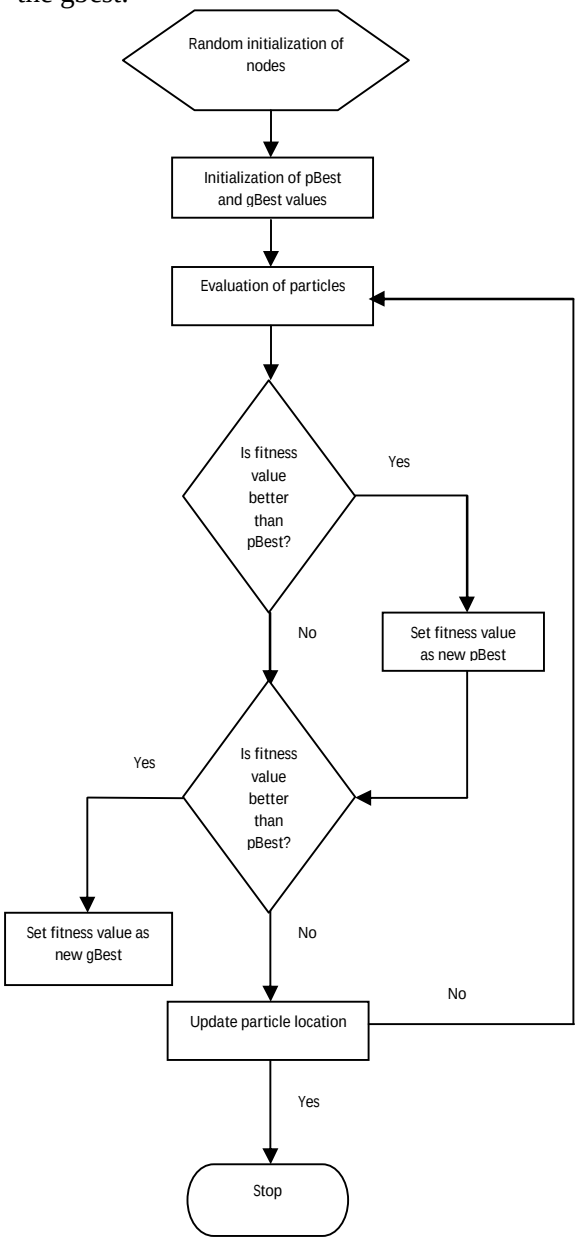

Figure 3: Working of PSO algorithm

$$V_i^{k+1} = wV_i^k + c_1\, rand_1(\ldots) \times (pbest_i - s_i^k) + c_2\, rand_2(\ldots) \times (gbest - s_i^k) \quad \ldots \quad (1)$$

The modification of the particle's position can be mathematically modeled according the following equation :

where,

v_i^k : direction of agent i at iteration k,
w: weighting function,
c_j : weighting factor,
rand : uniformly distributed random number between 0 and 1,
s_i^k : current position of agent i at iteration k,
$pbest_i$: pbest of agent i,
gbest: gbest of the group.

The following weighting function is usually utilized in (1)

$$w = wMax - [(wMax - wMin) \times iter]/maxIter \quad (2)$$

where,
wMax= initial weight,
wMin = final weight,
maxIter = maximum iteration number,
iter = current iteration number.

$$S_i^{k+1} = s_i^k + V_i^{k+1} \quad (3)$$

Application of PSO in several research areas has proved that results using PSO are faster and cheaper if compared with other techniques used so far.

4. Proposed Ids Architecture Based On PSO

In [21], authors have summarized various intrusion detection systems suggested by researchers based on topologies and attack types in mobile ad hoc networks. Considering the limitations of proposed techniques and dynamic nature of MANETs, we propose a distributed and cooperative intrusion detection system based on particle swarm optimization.
The model proposed contains five units. The local data collection unit records audit data of user and system activities. Local detection and evaluation engine will evaluate the patterns obtained with the attack signatures present in audit source unit. Whereas, cooperative detection and evaluation engine will check record and evaluate traces of network traffic network for any anomalies if present. Secure communication unit is responsible to allow or block the communication and also to inform other IDS agent in its radio range about the newly detected attack signature.
In this model, local and global optimization features can be effectively utilized. Individuality and sociality constants in the equation 1 (explained above) can be used to decide the threshold for attack signatures. It will be low cost and effective solution to dynamically changing environment of MANETs.

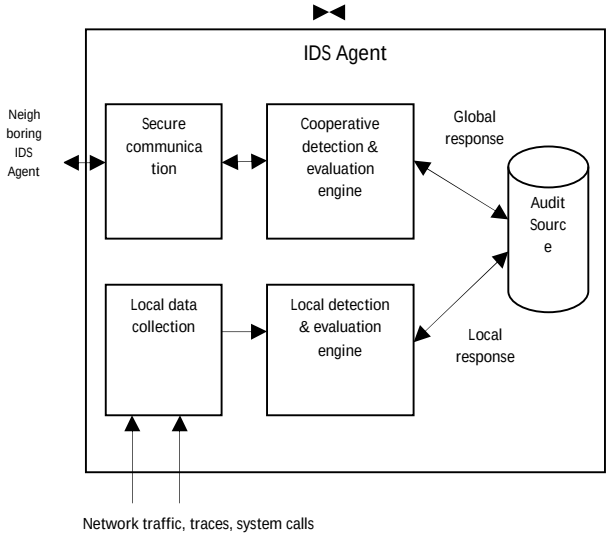

Figure 4 Architecture of proposed IDS using PSO

5. Conclusion

This paper summaries basics of IDS, challenges and attacks in MANET and briefly describes different approaches in Intrusion Detection Systems in MANET. Intrusion-Detection Systems aims at detecting attacks against computer systems and networks, in general, attacks against information systems. IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. As security is greatest issue in MANET, the paper can act as a source for the people who are trying to apply particle swarm optimization approach for intrusion detection.

References

[1] Surat Shrinoy,"Intrusion Detection Model based on Particle Swarm Optimization and support vector Machine", Proceedings of the Symposium on Computational Intelligence in Security and Defense Applications ©2007 IEEE

[2] Rodrigo Werlinger, Kirstie Hawkey, Kasia Muldner, Pooya Jaferian, Konstantin Beznosov , "The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?", Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, Pittsburgh, USA

[3] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", Proceedings of symposium on Computational Intelligence in Security and Defence Apllications © 2009 IEEE

[4] Zhao Chang, Wang Wei-ping, "An Improved PSO-Based Rule Extraction Algorithm for Intrusion Detection", International Conference on Computational Intelligence and Natural Computing© 2009 IEEE

[5] Zhang Vi, Zhang Li-Jun, "A Rule Generation Model Using S-PSO for Misuse Intrusion Detection", International Conference on Computer Application and System Modeling ©2010 IEEE

[6] Jing Ma, Xingwei Liu1, and Sijia Liu, "A New Intrusion Detection Method Based on BPSO-SVM", International Symposium on Computational Intelligence and Design © 2008 IEEE

[7] Tie-Jun Zhou, Yang Li, Jia Li**,** "Research On Intrusion Detection Of SVM Based on PSO", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding ©2009 IEEE

[8] Desheng Fu, Haibin Wang, "The Implementation of A Intrusion Detection System Model Based on Particle Swarm Reduction", ©2010 IEEE

[9] Liu-Hong Zhou, Yan-Hua Liu, Guo-Long Chen , "A Feature Selection Algorithm to Intrusion Detection Based on Cloud model and Multi-Objective Particle Swarm Optimization", Fourth International Symposium on Computational Intelligence and Design © 2011 IEEE

[10] Zhengjie Li, Yongzhong Li , Lei Xu, "Anomaly Intrusion Detection Method Based on K-means Clustering Algorithm with Particle Swarm Optimization", International Conference of Information Technology, Computer Engineering and Management Sciences© 2011 IEEE

[11] Ravneet Kaur, "Advances in Intrusion Detection System for WLAN", Advances in Internet of Things, 2011, 1, 51-54

[12] C. Kolias, G. Kambourakis, M. Maragoudakis ,"Swarm intelligence in intrusion detection: A survey", ©2011 Elsevier Ltd.

[13] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, "An Implementation Of Intrusion Detection System Using Genetic Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2 © 2012

[14] Chun-Wei Tsai , "Incremental particle swarm Optimization for intrusion detection", IET Networks., 2013, Vol. 2, pp. 124–130.

[15] WenJie Tian, Jicheng Liu, "A New Network Intrusion Detection Identification Model Research", Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference ©2010 IEEE

[16] http://www.windowsecurity.com/articles-tutorials/ intrusion_detection/IDS-Part2-Classification-methods-techniques.html

[17] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas **, "**An Implementation Of Intrusion Detection System Using Genetic Algorithm", , International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, 2012

[18] Srinivas Mukkamala, Andrew Sung and Ajith Abraham, "Designing Intrusion Detection Systems: Architectures, Challenges and Perspectives", © 2004

[19] Arun Kumar. R, Abhishek M. K, Tejashwini. A. I, Niranjan J. T, Pradeep R.P, "A Review on Intrusion Detection Systems in MANET", IJESIT, Vol. 4, 2013 pp. 609-618

[20] Rohit Kumar, Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications", IJCSE, Vol.3, 2012, pp. 121-125

[21] Tiranuch Anantvalee, Jie Wu, Wireless/Mobile Network Security, "A survey on Intrusion Detection in Mobile Ad Hoc Networks", Springer © 2006, pp. 170-196