International Journal on Advances in Engineering Technology and Science
Volume: 5, Issue: 1, 2024, e-ISSN: 2455-3131
DOI: 10.5281/zenodo.10718959

Intrusion Detection System Based on Particle Swarm Optimization in Mobile Ad-hoc Network: A Survey

Shruti Dixit[1], Navneet Kaur[2], Shalini Shahay[3]

Sanjeev Agrawal Global Educational University, Bhopal

[1]shruti.d@sageuniversity.edu.in

***Abstract*- Mobile Ad-hoc network (MANET) is the assortment of cooperative wireless nodes without existence of any access point or infrastructure. Due to problems like wireless radio, limited battery power, limited bandwidth and dynamic topology environment, nodes are susceptible for intrusion and attack. Security is an important field in this type of network. Each node in a MANET is capable of acting as a router. Routing and routing protocols are important aspects having various security concerns. The bio-inspired approach known as Particle Swarm Optimization (PSO) based on Swarm Intelligence (SI) is suggested for finding solution against attacks in the network. In this paper a survey of different types of attacks are presented and intrusion detection (ID) mechanisms based on PSO is discussed.**

Keywords- Mobile Ad-Hoc Network (MANET), Intrusion Detection Systems (IDS), Swarm intelligence (SI), Particle Swarm optimization (PSO)

I. INTRODUCTİON

In the 1990s, the concept of mobile wireless devices working together was proposed and the IETF established the Mobile Ad hoc Networks Working Group with the aim of standardizing routing protocols for MANETs [1, 2]. A set of wireless communication nodes performing self-configuration in a dynamic mode for the formation of network excluding fixed infrastructure or centralised supervision is termed asMANET. In addition to the role of a router, the nodes alsoplay the role of an end host. The routing protocol such as AODV [3] in such a network is authorized to determine the routes and provide communication among end points through intermediate nodes. The MANET is well liked and attractive since they offer good communication in the changing infrastructure for the applications such as rescue operations, tactical operations, environmental monitoring, conferences and the like. MANET research has been conducted on various aspects such as routing, security, quality of service, IP addressing, multiple access, and management of these networks. A significant part of the research work has focused on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer is vulnerable to attacks because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, and a lack of clearly defined physical network boundary and the transient nature of services in the network. PSO is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measureof quality. PSO technique is applied on IDS to overcome the problems in the network in terms of attacks.

The starting section of this paper discusses about IDS and classification of IDS for mobile ad-hoc networks. Later section discusses about major attack types ad-hoc wirelessnetworks and on different layers. Followed to which, detailed working of PSO algorithm is explained. Paper concludes with IDS based on PSO algorithm and researcher will getguidelines for further research.

II. INTRUSİON DETECTİON SYSTEMS

When a mobile node integrity, confidentiality, or availability is attacked by a set of actions intrusion prevention techniques can be taken into account [4, 5, 6]. ID is a method of identifying and responding to malicious and hostile activities targeted at computing and networking resources. Systems that are assigned to perform all the procedures related to intrusion detection are called IDS. ID in MANETs is more complex andchallenging than in fixed networks, because of the difficulty infulfilling the requirements of IDS.

IDSs achieve detection by continuously monitoring the network for unusual activity and taking direct preventive measures such as blocking a suspected connection. It can be run on each mobile node to check local traffic and local intrusions. Each node has local IDS that by this, node can connect to network and local IDS checking all send or receive data in/out node. There are three main components of IDS: data collection, detection, and response. The data collection component is responsible for collection and preprocessing data tasks: transferring data to a common format, data storage and sending data to the detection module.

The alarm part Intrusion detection can be classified into three broad categories: anomaly detection, signature or misuse detection, and specification-based detection. [7, 8, 9]

© 2016-2024, IJAETS

The first detection method examines the activity of the entire infrastructure for patterns of misuses known beforehand, usually referred to as "attack identities". On the opposite, anomaly detection approaches analyze the behavior of the protected system over time toward extracting an approximate estimation of what behavior is considered normal (or legitimate). A baseline profile of normal system activity is created. Any system activity that deviates from the baseline is treated as a possible intrusion. Specification based detection method describes the correct operation of a program or protocol. It sets the constraints and monitors the execution of the program with respect to the defined constraints. These two criteria have been associated with two performance evaluation variables: (i) Detection Rate (DR), which is defined as the ratio of the number of correctly detected attacks to the total number of attacks, and (ii) the False Alarm Rate (FAR), or false positive rate, which is the ratio of the number of normal connections that are misclassified as attacks to the total number of normal connections. An IDS maintains high detection rates and false alarm rates as low as possible

III. MAJOR ATTACK TYPES OVER MANET

MANETs are more susceptible to security attacks than existing conventional networks due to lack of trusted centralized administration, limited bandwidth, limited power, wireless links, dynamic topology and easy eavesdropping. [5] A security protocol for ad-hoc wireless networks should satisfy the following requirements: Confidentiality, integrity, availability and non repudiation. Hence designing a foolproof security protocol for ad-hoc wireless is a challenging task. An attacker can violate them by passively or actively attacking on MANETs. Hence it can be classified into two major categories, namely, passive attacks and active attacks. A passive attack are not disruptive but are information seeking which may be critical in the operation of a protocol, while an active attack may be directed to disrupt the normal operation of a specific node or target the operation of the whole network of a MANET. The attacks can be classified further into two categories external attacks and internal attacks. External attacks are the comprised nodes which are away from the network. Internal attacks are from the comprised nodes that areactually part of the network.

Table I Attacks on Ad-Hoc Wireless Networks

Type of attack	Characteristics	Examples
Passive attack	Obtains information withoutdisturbing normal network operation Difficult to detect The attacker does not send any message, just listens to the channel	Traffic analysis, Traffic monitoring eavesdropping
Active attack	Can disturb network operation by modifying or deleting information injecting false message or impersonating a node Can be internal (attacker within the network) or external (attackeroutside the network)	Modification, impersonation, fabrication, jamming and message replay

TABLE II Attacks on Different Layers

Layer	Type of attack
Application layer	Repudiation
Tranport layer	Session hijacking
Network Layer	Wormhole,
	Black hole, Gray hole,
	Byzantine,
	Sybil
	Resource Consumption attack
	Rushing attack
	Information Disclosure
	Routing attacks: Routing table overflow,Routing table poisoning
	Packet replication
Multiple Layers	Denial of Service (DoS),Impersonation, Device tampering
MAC layer attacks	Jamming

IV. PARTİCLE SWARM OPTİMİZATİON (PSO)

In PSO, any node in a MANET dynamically discovers a route to any node. Initially nodes are identified by sending a route request signal RREQ. After receiving route request, any node equivalent to swarm particle initialized position and velocity using the concept of PSO [10, 11, and 12]. In PSO animals wander through a 3-dimensional space, in a search of food and these algorithms make use of particles moving in an n-dimension space to search for solutions for an n-variable function optimization problem. Particles are individuals and thepopulation is called a swarm. The initial swarm is generally created in such a manner that the population of the particles is assigned randomly over the search space. At every iteration, each particle is updated by two 'best' values, called pbest and gbest. In the problem space, each particle keeps track of its coordinates, which are associated with the best solution (fitness) the particle has achieved so far. This fitness value is stored, and called pbest. When a particle takes the entire population as its topological neighbour, the best value is called gbest global best value. Steps in PSO algorithm are briefed as below:

Initialization of swarm by assigning a random position.

Approximation of the fitness functions for each particle.

For each individual particle, compare the particle's fitness value with its pbest. This pbest is compared with the present particle's position. Updation of pbest is possible if the present particle's position is better than the pbest value, then pbest is set with the present particle's position, xi aspi.

The particle that has the best fitness value will beidentified as gbest fitness function.

Modification of velocities and positions of all the particlesusing (1) and (2).

Repeating steps 2{5 until a sufficiently good fitness valueis achieved.

The movement of the particle is governed by updating itsvelocity and position attributes according to following equation:-

$V^{t+1}_i = wV^t_i + c_1r_1(x_{pbest} - X^t_i) + c_2r_2(x_{gbest} - X^t_i)$….(1) $X^{t+1}_i = X^t_i + V^{t+1}_i$… (2)

w= inertia weight;

c_1= cognitive acceleration coefficient, c_2= social acceleration coefficient,

r1 and r2 are the random values between 0 and 1,

xpbest is the personal best of the particle and xgbest is the global best of the particle. X^t_i is the current position of i^{th} particle at iteration t. V^t_i is the velocity of i^{th} particle at iteration t. In standard PSO, a minimization problem is considered which tends to defined a parameter set x a vector of m decision variables: $x = (x_1, x_2 \ldots x_m)^t$ for single objective

i.e. Minimize/Maximize f(x); subject to

$x_{i(LB)} \; x_i \; x_{i(UB)}$; i = 1, 2, …, m

even birds and fishes appear to have very limited intelligence as individuals. [13]

A new intrusion detection system called Enhanced Adaptive Acknowledgment (EAACK) [14] especially designed for MANETs is proposed. It is compared with existing approaches and results a higher malicious behaviour detection rate in particular circumstances. In the case of receiver collision, limited transmission power, and false misbehavior report, the results are excellent against Watchdog, TWOACK, and AACK. This scheme incorporates digital signature in order to prevent the attackers from initiating forged acknowledgment attacks. The DSA scheme is more suitable tobe implemented in MANETs and it can vastly improve the network's PDR.

[15] The quality of service of the network is enhanced in terms of packet loss by exclusion of Black hole node from route establishment process. Each node trust value is calculated and this value will be increased depending upon theability to forward packet and ability to forward route request. At the time of route discovery if alternative trusted nodes are available, it will always try to establish a path where more trusted nodes are involved. Here the route establishment is done according to the calculated trust value saved in the routing table rather than the traditional shortest path. 10 10LB= Lower bound of variablesU B= Upper bound of variables

V. LİTERATURE SURVEY

In recent years, the research in the area of Computer Networks& Internet is increasing with leaps and bounds. Each one of these networks has proven to hold its own security inefficiencies and vulnerabilities. As traditional approacheslike antivirus, firewall, spyware & authentication mechanism fail to provide security to large extend. Some interesting solutions like Intrusion Detection & Prevention Systems have come into picture, but these too have some problemsresponding in real time. PSO algorithm is used to find out solution for the above problems. It is a computation intelligence technique, which was motivated by theorganism's behaviour such as schooling of fish, flocking of birds and colonies of ants. PSO algorithm is able to give solution for difficult optimization problems. Different approaches for an IDS based on PSO are elaborated.

An ID is a problem of great significance and nowadays become a necessary component of almost every security infrastructure. Many different approaches have been defined in order to increase the efficiency of IDS. The term Swarm Intelligence (SI) was first introduced by Beni 1989. Methodologies, techniques and algorithms based on SI, a new bio-inspired research field attracts attention from the behaviour of insects, birds and fishes, and their unique ability to solve complex tasks in the form of swarms which is impossible in individual level. Indeed, single ants, bees or [16] A swarm based efficient distributed IDS for MANET was proposed. The nodes with highest trust value, residual bandwidth and residual energy act as a active nodes. The trust value is collected from all monitored nodes by the each active node. The active nodes adaptively change as per the trust thresholds. If the active node finds any node below a minimum trust threshold, then the node is marked asmalicious, during collaborative exchange of the trust values ofthe monitored nodes among the active nodes.

[17] This paper proposed a novel approach for enhanced intrusion detection system for malicious node to protect against attacks in ad-hoc on-demand distance vector routing protocol. It leads to identify malicious node, less conservation and less communication breakage in ad- hoc routing. Thisapproach has been found advantageous for identifying malicious nodes in black hole attack, neighbour attack, sequence number attack and packet forwarding attack up to 700 nodes.

A survey of preventing and identifying Black hole attack using trust management mechanism in MANET is proposed [18]. This attack has serious impact on routing and delivery ratio of packets. A trust-based routing, intrusion detection system, sequence number comparison and Data Routing Information table (DRI) techniques are used to avoid black hole attack. Trust based On Demand routing mechanism identifies and decreases the risk by malicious node in the path. An Artificial immune

system (AIS) based security model Bee AIS for a Bio/Nature inspired MANET routing protocol known as, Bee Ad-Hoc is proposed [19]. Its performance is compared with a cryptographic security framework, Beesec. The results of our extensive attack simulations verify that a malicious node can seriously disrupt the routing behaviour of Bee Ad-Hoc protocol. However, Bee AIS can successfully detect the non-self-antigens and drop them to counter theattacks. It provides security at no additional control or energy costs to the system.

A new secure power-aware ant routing algorithm (SPA-ARA) [20] for mobile ad hoc networks based on ant colony optimization (ACO) algorithms. It is a swarm intelligent technique which introduces a new metric, next-hopavailability. It models the probability to find the best availablenext hop to be taken by the reactive ant and data packets to reach the destination, which is a combination of two metrics.It offers a good balance between selection of fast paths and a better use of network resources by enhancing path availability and reducing travel time of packets. Unauthorized and compromised nodes in MANETs are detected by incorporating a protocol based on trust model.

[21] The grammatical evolution and genetic programming techniques for detecting ad-hoc flooding and route disruption attacks on AODV has been applied. Authors showed that their evolved programs performed good on simulated networks with varying mobility and traffic patterns. This methodology is not applicable to WSNs where sensor nodes have limited capacity for data processing and storage. It is applicable for MANETs where most of the nodes (e.g., PDAs) are powerful enough to run such energy consuming algorithms.

[22] The proposed method identifies the attack and provides the noble solution for attack by using the fuzzy logic technique. The system also contains IPS mechanism techniquewhich gets input from fuzzy technique and provides the secure data communication over the network. It also monitors for the traffic of black hole and gray hole attacks. Efficiently detects the attack when compared to existing method.

Machine learning techniques like Neural Network (NN), Support Vector Machine (SVM) and Rough Set etc. wereproposed for making an efficient and Intelligent Network IDS. This work investigated that in order to secure the network with a single technique proves to be insufficient to prevent from ever increasing threats. So, there is an immediateneed to combine all security technologies under a complete secure system that integrates the strength of these technologies. In this work, researchers have combined PSO and its variants with various machine learning techniques used for anomaly detection in network IDS so as to enhance the performance of IDS. [23]

[24] K-means is a popular anomaly intrusion detection method to classify unlabelled data into different categories but suffering from the local convergence and high false alarms problems. In this paper, two soft computing techniques, fuzzy logic and swarm intelligence, are used to solve the above problem. SFK-means algorithm is proposed, in which Fuzzy K-means and Swarm K-means solve the local convergence problem and the sharp boundary problem respectively. Results of experiments on dataset KDDCup99 show that proposed method can be effective in detecting various attacks.

[25] Cryptography based SAODV and trust-based TAODV, two MANET routing protocols are compared. The results of implementation and evaluation of both protocols on real resource limited hardware are discussed. It is concluded that by taking advantages of both routing protocols, a new secure hybrid protocol can be developed.

The research papers are discussed with advantages and disadvantages as listed in the table III

TABLE III Advantages and Limitations

Sr. No.	Approach	Advantages	Limitations
1.	QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack [15]	Higher threshold values give less packet drops providing more reliable communication	Trusted routes are considered rather than shorter route. The routes may be longer. Less number of nodes are considered.
2.	A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET) [16]	Reduction in energy consumption and cost involved in the monitoring process of malicious nodes.	Performance is compared with only one technique. Less no. of nodes is considered.
3	Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption [18]	Identification of malicious nodes with less communication breakage and less conversation. Large no of nodes upto 700 are considered.	Nodes having large energy consumption are not considered.
4.	Fuzzy Based Intrusion Detection Systems in MANET [22]	Identifies the type, the range and extension of attack. There is no change in the value of packet delivery ratio and the packet drop with and without attack.	The fuzzy logic technique is used and jitter value obtained is more.
5.	Cryptographic versus trust-based methods for MANET routing security [25]	Provides new direction for development of new trust metrics for ad-hoc networks	Tools are computationaly very expensive

VI. CONCLUSİON

MANETs are prone to a variety of attacks that primarily target the protocols of the transport, network and data-link layers. IDS aim to detect attacks on mobile nodes and intrusions into the networks and attack against information systems. ID based system works as a guard system that automatically detects

malicious activities within a host or network. This work offers a comprehensive analysis of the internal mechanisms of PSO based IDS approaches. The limitations and advantages of different approaches are discussed. The paper inspires open research issues in the field of intrusion detection mechanisms based on PSO. PSO based routing algorithm is morepromising for specific nature of ad-hoc networks and outperforms in real scenarios/constraints/environmental conditions and gets an efficient and effective routing protocol for MANET.

REFERENCES

[1] Siva. R.M, C. and B. S. Manoj, "Ad-Hoc Wireless Networks: Architecture and Protocols", Pearson, USA, 2004.

[2] E. Royer and C. K. Toh, "A review of current routing protocols forad-hoc mobile wireless networks", IEEE Personal Communications, 1999

[3] Sheng Liu, Yang Yang, Weixing Wang, "Research of AODV Routing Protocol for Ad Hoc Networks", Conference on Parallel and Distributed Computing and Systems, Elsevier 2013, pp. 21-31

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

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

[6] Ansam Khraisat , Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges", Cybersecurity 2:20 https://doi.org/10.1186/s42400-019-0038-7, 2019

[7] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, Farhan Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", wileyonlinelibrary.com/journal/ett 1, 2020.

[8] A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness, " Iot intrusion detection system using deep learning and enhanced transient search optimization," IEEE Access, vol. 9, Article ID 123464, 2021.

[9] F. Alghayadh and D. Debnath, "A hybrid intrusion detection system for smart home security based on machine learning and user behavior," Advances in Internet of Things, vol. 11, no. 01, pp. 10–25, 2021.

[10] James Kennedy and Russell Eberhart, "Particle Swarm Optimization", IEEE, 1995

[11] G. Di Caro, F. Ducatelle, L. M. Gambardella, "Swarm Intelligence for routing in mobile ad hoc networks", In Proceedings of the 2005IEEE Swarm Intelligence Symposium, SIS 2005, 2005, pp. 76–83

[12] S. Lalwani, S. Singhal, R. Kumar and N. Gupta, "A Comprehensive Survey: Applications of Multi-Objective Particle Swarm Optimization (MOPSO) Algorithm", Transactions on Combinatorics, Vol. 2, 2013, pp. 39-101.

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

[14] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE transactions on industrial electronics, vol. 60, no. 3, march 2013.

[15] Radha Krishna Bara, Jyotsna Kumar Mandalb and Moirangthem Marjit Singh, "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", International Conference on Computational Intelligence: Modeling Techniques and Applications, Elsevier, 2013

[16] G. Indirani and K. Selvakumar , 'A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)' International Journal of Parallel, Emergent and Distributed Systems, taylor and francis ,2014, Vol. 29, No. 1, 90– 103

[17] I. Raza, S. A. Hussain, "Identification of malicious nodes in anAODV pure ad hoc network through guard nodes", ACM Comput. Commun., 2008, 31, (9), pp. 1796–1802.S. Umang,

[18] B.V.R. Reddy and M.N. Hoda, "Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption', The Institution of Engineering and Technology 2010, Vol. 4, Iss. 17, pp. 2084–2094 doi: 10.1049/iet-com.2009.0616

[19] Nauman Mazhar and Muddassar Farooq, "BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc", BeeAIS: AIS Security, Springer, 2007. pp. 370–381

[20] Shabana Mehfuz and M. N. Doja, "Swarm Intelligent Power- Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications Hindawi Publishing Corporation, 2008

[21] S. Sen and J.A. Clark, "Evolutionary computation techniques for intrusion detection in mobile ad hoc networks", Elsevier J. Computer Networks, vol. 55, num. 15, pp. 3441–3457, 2011.

[22] Vishnu Balan, Priyan M K, Gokulnath, Usha Devi, "Fuzzy Based Intrusion Detection Systems in MANET", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Elsevier, 2015, pg. no. 109 – 114

[23] Khushboo Satpute, Shikha Agrawal, Jitendra Agrawal, Sanjeev Sharma,"A Survey on Anomaly Detection in Network Intrusion Detection System Using Particle Swarm Optimization Based Machine Learning Techniques", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer , 2013 ,pg. No. 441- 452.

[24] Roya Ensafi, Soheila Dehghanzadeh, Mohammad -R. Akbarzadeh, "Optimizing Fuzzy K-means for network anomaly detection using PSO", IEEE/ACS International Conference on Computer Systems and Applications, 2008

[25] Jared Cordasco, Sussane Wetzel, "Crytographyic versus trust-based methods for MANET routing security", Elesevier notes theor. Comput. Sci., 2008, 197, pp. 131-140