Indian Journal of Science and Technology, Vol 9(11), DOI: 10.17485/ijst/2016/v9i11/89264, March 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Survey on Intrusion Detection System: State of the Art Review

J. Amudhavel[1]*, V. Brindha[1], B. Anantharaj[2], P. Karthikeyan[1], B. Bhuvaneswari[3], M. Vasanthi[1], D. Nivetha[1] and D. Vinodha[1]

[1]Department of CSE, SMVEC, Pondicherry - 605107, Tamil Nadu, India; info.amudhavel@gmail.com, brindhavenkat10@gmail.com
[2]Department of CSE, TCET, Vandavasi - 627425, Tamil Nadu, India; ananthu_arun72@yahoo.com, mails2karthy@gmail.com, vasanthi.saraswathy@gmail.com, nivethadjeacoumar@gmail.com, vinodjeacoumar@gmail.com
[3]Department of CSE, Pondicherry University, Pondicherry - 605014, Tamil Nadu, India

Abstract

Background/Objectives: To analyze and monitoring the activity of nodes using an IDS Intrusion Detection System which provide security to the system. **Findings:** In this research, a network building was made with simple node formation with a fitting technique. So that it is easy for a user or beginner to understand the asymptotic dominion factors, due to the wide growth of nodes on network. Intrusion detection system is made of several nodes. These nodes are grouped and combined as a network. Since each node in a network has unique characteristics they may have high chance of attack from malware during the communication between systems. **Applications/Improvements:** Network of topology is done by creating and connecting various sub networks. Sub networks traffic is cleared and monitored with the package of IDS. It works on synchronous message transfer mode which provides acknowledgement to sender and receiver. All sub networks is managed by its corresponding system and further provide update to the master node on the network. Due to this broadcast of messages all other nodes may be in safe state of avoidance from attacker.

Keywords: Ad-Hoc Network, Conversation Exchange Dynamics, Intrusion Detection System, Intrusion Prevention System, Network Security

1. Introduction

An IDS (Intrusion Detection System) monitors the activity of the node. IDS are used to observe and assess the network in order to locate the attacks in a corporate network. An ISD provides confidentiality, security and ultimate availability of resource to an organization. Intrusion detection consists of two major classifications they are signature based and heuristic intrusion detection system. The heuristic based method is also called as anomaly based intrusion detection system[1]. For the purpose of data storage and retrieval of data a database and data mining is been used in the concept of intrusion detection. In which a device store certain data's and the data's are first inserted or implemented in a database. These retrieval and storage are automated with accuracy. These data mining tool are provided to accurately capture the actual behavior intrusion system. For these activity numbers of data extracting algorithm is evolved to compute models. Fuzzy rule-based classifiers are introduced to make decision so that it is considered as a power full tool. Intrusion Detection System is a basic and fundamental concept of all system and network[2].

An IDS is widely evolved in organizations due to the additional layer of security provision. It has been evolved from firewalls. Simply, firewalls are the predecessor of IDS. Even though firewall provides security, it has many shortcomings. In order to replace the technique an IDS is produced. Firewalls only prevent the unauthorized entry into network in an organization. But IDS provide both

*Author for correspondence

the storage and prevention of data. An industrial network is managed with the use if Distributed Intrusion System. In order to manage the distributed system a MANET technique is been evolved to examine the difficulty of distributed intrusion detection system[3]. The concept is classified into two categories one is by hypothesis and another is made practically.

On hypothesis or theoretical view, it is proposed with the average improvement rate of detection under very balmy state. Then the next part is by describing it practically with the advancement of clustering algorithm. Since the cluster algorithm is used, it is necessary to update the centers of clusters and machine learning concept such as artificial neural network. It creates index for anomaly computing held locally. Data centralization, Multi-class classifications are some of the condition used. Some of the assumptions are violated in MANET[4]. In general the nodes of MANAT are separated and are connected via wireless links. MANET is a kind of routing and the process is under the development. Those tasks are managed along signature based intrusion detection system. Some processes are evaluated under certain patterns. Patterns are well defined to involve in process. MANAT's are constructed with a group of tens and hundreds of nodes. Network building made with simple node formation with a fitting technique.

It is easy for a user or beginner to understand the asymptotic dominion factors, due to the wide growth of nodes on network. Intrusion detection system is made of several nodes. These nodes are grouped and combined as a network. Since each node in a network have unique characteristics they may have high chance of attack from malware and malicious attacks during the communication between systems. On account of these issues, network based (IDS) is launched termed as NIDS[5]. It is used on a group of network with different constitution and divergent environment for the purpose of augment the network security. As discussed above, there exist two categories: signature based and anomaly based[6]. By using NIDS, the process performs the election technique on an essential network. By performing these skills, a lightweight detector is deployed to serve and capture the freight on network.

2. Motivation

The fundamental need of the entire network is considered as IDS. All the evolving technology is made use of IDS. For an instance, a defense environment is considered. In which all the soldiers should be active and act according to command of the general. Here not only a schedule is maintained but also a secured way of communication is obtained[7]. Likewise, all the nodes in a network must be active and as well as provide a secured communication throughout a network. To achieve the good security level. IDS is employed over the entire network. IDS has a utility of providing additional layers on the account of securing an organizational context. Authentication is descripted with firewalls; they prevent the entry of unauthorized personal into the organizational network. As the entire message communicates[8] through a network, obviously there exists network traffic. They are lessening by widely distributing the resource and service. This is done by network topology by creating and connecting various sub networks. Sub networks traffic is cleared and monitored with the package of IDS. It works on synchronous message transfer mode provides acknowledgement to sender and receiver. All sub networks is managed by its corresponding system[9] and they provide update to the master node on the network. Due to this broadcast of messages all other nodes may be in safe state in avoidance from attacker. It is not enumerated that the affected node is to be liberated from the network. Instead the node is placed as ideal until a set of process to be completed. Each and every local sub network is watched by its clone. Whenever an abnormal activity is found on a network the IDS alert the entire devices that are connected with each other. It reports about issues to the corresponding intrusion detection system. This process is carried out to check whether other part of the network is reliable[10]. Here we interconnect many systems and it is processed in the order of network. Hence interconnection security should to consider as most important factor due to the exchange of data in well secured manner by using various communication and security protocols.

3. Contributions

One of the wide areas of IDS is network intrusion detection system. It has many critical issues and pretentious like malware over a large and whole network. To move over from the hackers and unreliable environment, NIDS is used to propagate the network with high security, availability with the aim of enhancing security in network. An adaptive based character frequency is discovered in the signature based NIDS method. This helps to speed

up the ability and performance due to performing simple signature matching process over a distributed environment. [11]Distributed network environment describes its application in constructing a packet filter. To avoid implementation issue and improve the flexibility of scheme, further model is proposed to constructing a packet. There by enable to correspond with the signature based NIDS, provided if the application is specified with packet filters. To avoid the run time attacks and to improve the reliability, some of the updating is made on signature based NIDS. Commonly as like simple IDS scheme NIDS also consist of many small nodes grouped together. These all make the formation of sub network, and then all sub networks are managed by a single master or agent over a huge network[12]. The agent node communicates with other nodes with the leading analysis that provide high level lattice management.

4. Organization

The other concept of the discussion is classified according to their sections. Design module is discussed in section 2 with two subparts. Section 3 mentions the concept deployed in system. Section 4 mentions its security factors. Section 5 enumerate about divisions that are made in IDS. Section 6 narrates about Distributed Intrusion Detection in MANET. Section 7 represents the Distributed intrusion detection system. Sections 8 consist of related works. Section 9 deals about the conclusion.

5. Design

The design of Intrusion detection is divided into two basic steps. An audit records called as review or analysis is created, initially. The next stage evaluates audit record with mutual exclusion of intrusion inception. Audit trail is referred as main element that describes the entire created audit trail under it. In further steps regular checking of network is done for all activities that have been over limit the indicated threshold value. At last an Intrusion Detection repot is broadcasted for review and that are viewed by system administrator in order to achieve potential break. Figure 1 deals with the discussion which is made on techniques and stream that are involved in IDS; they are the main techniques is Distributed Intrusion Detection System. It makes use of MANET's for wireless transmission through nodes in a network. Intrusion Prevention System prevents the data form

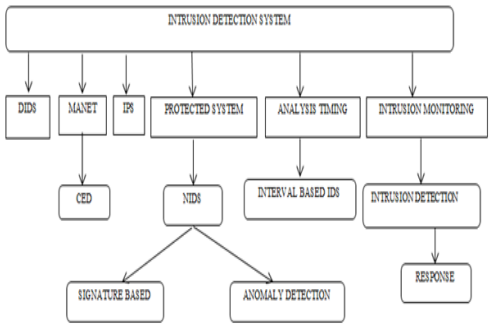

Figure 1. Techniques in IDS.

unauthorized parties, hacks. Then the protected system is evolved (NIDS) with signature based and anomaly based. The most important factor is time analyses that are made by interval based IDS. The monitoring is done at regular intervals by analysis then the intrusion is detected on a network called intrusion detection and the response is made after the notification.

DIDS: Distributed Intrusion Detection System.
MANET: Mobile Ad-Hoc Network.
IPS: Intrusion Prevention System.
CED: Conversation Exchange Dynamics.
NIDS: Network Intrusion Detection System.

5.1 Concepts

Many organization and financial institute involve in storage of confidential data. For that purpose audit records are used. They are referred under security based chronological method. Audit records are simply defined as a succession of paperwork as an abstract and validate or invalidate the data's that is to be transferred over the network[13]. It has been defined that the strategy needs some identification about the constitution of mismatching behavior. They are made automatically by detecting activity that is to be occurring. In case of habitual network like online transaction the network may to huge are light. Obviously, IDS is mutually written to the size of network according to product based market and its traffic for a particular model of strike. So therefore every vendor based on IDS should be notated with the signature for the known assault. Various kind technology is been evolving in IDS in order to increase the ability of networks. All data's evidently cross the open system interconnection simply layers of OSI[14]. Hereof all the data will be converted and broadcasted in the form of stream of bits, packets with its source and destination code. By the

protocol analysis content searching and exhale thousands of worms. In real time environment every part of the network should be attached with a detector. Snort has been considered as a pioneer of NIDS. But of far greater significance Snort consist of many versions and it update trendy data promptly.

5.2 Security

As the use of internet connectivity is being increasing the threats and Denial of Service (DOS) also increases accordingly. In other words, the filter provides an additional round of signature matching for signature-based NIDSs. Only when the exclusive signature matching is failed, a packet can be sent to the NIDS. Thus the filter can reduce the burden of a NIDS without upset the whole network security.

5.2.1 Security Onion

After the reference of security factors, a term is defined as security onion that is mainly involved in distributed nodes. That being the case, IDS activity is performed over all the layers of data conveyance. It leads to the development of some other tools. This factor is possible only in the case of IDS with single host and multiple nodes.

5.2.2 Bro IDS

This is similar to security onion with small dissimilarities in dependency between systems. Whenever a node in a network is identified with attack the changes and behavior will propagated to alternative clone. Thereof it has many trend improving advantages over it.

From Figure 2, it is explored that the structure of security has ingredient with simple blocks. Initially an internet is established with its Ethernet and IP address. Then other resources like printer, system, email server, file server are connected to Ethernet channel. They are grouped and joined together with firewall to get a secured network.

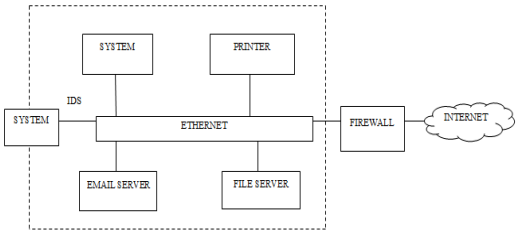

Figure 2. Intrusion Detection System in a network.

6. Classification of Intrusion Detection Systems

IDS have major six representations as according to its behavior. An attack is traced by monitoring the behavior of every profile with its security constraints. This is done with matching patterns as like signature based. It spots the area where leakage is present in network. In some cases user may be ideal in a network after accessing a service. Therefor service may be directed to other client. It manages resource of a system.

7. Distributed Intrusion Detection in Manets

Mobile Ad-Hoc Network (MANET) is more sensitive to the attacks than the wired network infrastructure since it contain a very limited physical protection constrain. Routers are evolved in order to make interaction with other nodes. A cell in a node is initially initiated and corresponding information is transmitted to other layers. From one base station waves are forwarded to next area. In some cases it may be overloaded due to network traffic. The process made here is to defending MANAT's against attacks, hackers of computer environment.

8. Distributed Intrusion Detection System

A Distributed Intrusion Detection System (DIDS) is established by dint of grouping of many IDS over a large set of network. By applying centralization method of communication we can establish communication between single server and with multiple clients. Server contains a separate database and connected to different clients through a socket. It is in practical and necessary to fix many IDS on the path of network. The path is created with routers. These routers select a path to transmit data. If data is not sending properly, it can be achieved by fast rerouting concept. The data's will be sending back to router and it will establish a reliable path for a packet of data. There exists a time monitor. The main use of DIDS is to detect intruders over a network. For an instance many of the security issues are occurred by interior personalities. Even though they have authority to access a service they may cause some security problem unknowingly. So that internet is initially protected by firewalls and then

connected to IDS. So that user activities and behavior are noted by DIDS. By following this technique, area of access can be partitioned according to their position of work. DIDS server is practical to web interface to permit corporate members to the upper part of technology to update the prevalent attack of data.

9. Related Works

Intrusion Detection (ID) is a type of security for managing system from computers attacks. An Intrusion Detection System (IDS) is a process that analyses what happens in a system during an execution and then tries to find indications that the computer has been misused by unauthorized users. Intrusion Detection systems are developed in an action of response to the increasing number of attacks on major computers and networks.

Discussed mainly about fuzzy rule to detect attacks on a network[15]. Fuzzy rule are introduced with three rules to detect intrusions in a network. They are then compared with other machine learning techniques like support vector machines decision trees, and linear genetic programming. Further the Distributed Soft Computing-based IDS (D-SCIDS) are maintained as a combination of different classifiers to model lightweight and more accurate (heavy weight) IDS. Experimental results clearly show that soft computing approach play a major role for intrusion detection in a system. These techniques are framed for DIDS and use numerous soft computing paradigms. It is deled with light weight and heavy weight intrusion detection system. Hybrid architecture is proposed. The fuzzy classifier provides 100% accuracy. Enhance performance of other soft computing paradigms. Snort is an existing system that states as a open source network intrusion detection and prevention system. It continuously uses additional resources in the system. And the technique in brief, it consists of more detection and transmitting process. It will be more efficient when it has high extensibility and reliability. Some of the suggestion to overcome is by using three fuzzy rule based classifiers is mainly discussed. Hence the time and accuracy in detection process should be in better way.

Proposed the concept about the practice of Conversation Exchange Dynamics (CED) for the combination and display of the information about sensor from multiple nodes in a network[16]. The theme consists of many sensors, reporting to individuals to find a central server for aggregated analysis. Different consequences of network attacks and intrusions were intended to study the efficiency of the distributed system. It is exposed to different mixtures of network attack in a system. And the techniques explored are conversation exchange dynamics between groups. Here a ball and bucket concept is used to represent conversation and information. A decision tree is defined with four buckets. It detects a global attack. This concept is evolved from the approach that the Intrusion detection on network traffic sensor. Forwarding the information that is sensed and sends back to the central process. Detection of path used to transfer the information effectively. Some disadvantages such as the scope of attack is more. Due to wide spread it infect the computer host and it is self-replicated. It allows connection between uninfected hosts to infected host.

Has proposed some concept about the distributed performance in mobile Ad-Hoc Network and deals with its problem[17]. A hierarchical system provided with three levels is used for collection of data, processing and transmission. To collect the raw data of network operation a local intrusion detection system are involved to each node of the MANET. A local anomaly processes the discrepancy between the present nodes. It also describes about the clustering algorithms for computation. Techniques they done are IEEE 802.11protocol and OLSR routing schemes. The main advantage is by Contributions of practical and theoretical nature is presented. Detection of Accuracy is high in cluster level. Iodation and extendibility are high. Some of the disadvantages can be overcome by the better technique the speed and extendibility should to increase. Sensor node manager can be introduced to get successful transmission.

Has produced the concept about the scheme and application of a two-stage intrusion detection system[18]. Intrusion detection is delivered by investigating the framework from the application-level connections of network. A fixed set of behaviors is determined disconnected, and these behaviors are traced vigorously during the process of the network. Techniques they used are Network and detect models describes the architecture, spoofing, jamming. The application layer is to make connection between various network aware applications. The main advantages are the security and safeguards properties of a specific or a group against risk. It is a well embedded system that consumes low power, low memory. It will be better by adding the concept Instead of only using ad-hoc and sensors. Routing algorithm may be included. It will be effective while it allow developing real time applications.

Improved the performance of signature-based by decreasing the time consumption of signature matching. In addition, constructing a ACF-EX based packet filter is also achieved[19]. The proposed work is to advance an ACF-EX signature matching pattern for a signature-based NIDS with the resolution of speeding up the process of signature matching in a network distributed environment, and describe its application in constructing a packet filter. The signature matching limit and subordinate the presentation of a signature-based NIDS in a large-scale network situation and in which cost is least to input. The performance of our scheme can be made more effective by using much more parameters. It should effectively predict and measure the network situations from the data delivered between NIDS agents and the central analysis server.

Proposed an automated device that translates CPN that requires IDS design into software intrusion detection managers in MAIDS[20]. The proposed techniques are done with the translator to adapt model intrusions into the CPN for IDS design; this implement can repeatedly produce intrusion detection software agents from a high level report of interruptions. CPN has been widely used to model difficult and distributed systems. If the CPN to agent's conversion are done manually, it is complex to make such a contention. Simplicity of notifying MAIDS to detect new attacks is significant since new interruption types arise every day. To overcome todays[21] attacker problem we have to merge indications based on other data such as user identifiers so the relationship of events among machines can be more active.

Discussed about an agent-based approach to make a successful mechanism for a distributed ids by artificial immune system[22]. This paper maintains an agent-based approach to make a successful mechanism for distributed IDS by AIS. The AIS paradigms are negative selection, clonal selection, danger theory, and immune network. The proposed[23] MAIS-IDS have advantage of higher recognition accuracy by collaboration between virtual machines than individual works. Future studies will evaluation MAIS-IDS in an environment with high loading and complexity that approximates the real environment. Agent features will be increased and optimized and the system will be implemented using a real IDS.

Discuss about a data provision for distributed IDS and the distinctive tasks tackled using distributed intrusion detection systems is to share and in what way to part data[24]. In this Projected an outline for distributed detection systems[9] and the method is to improve the trade-off among the period essential to notice an intrusion, and the capacity of message between the distributed IDS. The central recognition[25] method suffers from scalability difficulties owing to this central block, and makes itself a goal of an attack. Naive method to this problem moderates the quantity of indication that is offered to every system, thus growing the danger of missing an incident, projected a distributed detection system to notice indicator attacks. Better techniques should be added to overcome the problem in information sharing.

10. Challenges

Intrusion detection system[26] is a system that detects malicious attacks from attacks and report to the administrator. They had come across some limitations in implementing many approaches. Networks are secured from attacks by managing the ids in each system that are maintaining. More challenges are proposed to overcome the limitation. The solution proposed in this paper[27] is to maintain and develop a security policy at three levels. This is an exciting new method that proposes new methods appropriate for those liable for safety and improves network security.

The first security level of intrusion detection is to exercise an intrusion detection system using an eminent traditional approach with the benefits of the above approaches[28]. It will be sited in firewall to avoid network attacks from outside hackers by denying malicious connection shots by unauthorized users from outside. We propose a Network based Intrusion Detection System (NIDS) using a process of database attacks. The foremost benefit of a system based on information is that it typically produces very limited false positives and its restriction is that it cannot detect any new intrusions that do not occur in the database of attacks. This problem will be enhanced in levels two and three, which will mainly help the process to detect any new attacks that affects computer. The investigation of these attacks will support us to update our database attacks in a system.

The second level of intrusion system detection[29] is to state efficient security policies, in which the security are based on the responsibilities given to users in the concern by the separation of the system to Virtual Local Area Network and the practice of Access Control List. The main impartial of this level is to guard the interior system by malicious core users may misuse their insider attacks and forwards that spread from the external and penetrate systems by external attacks.

The third level of security policy[30] is to define a security working through a device that relates the information in the angle of access control to the concern and the data from the list of logical access control peoples to the user. This means, deny network access to users who are not actually operational of the company at this time. This control will prevent identity usurpation from inside or from outside to the internal computer network. These levels of our intrusion detection system can automatically detect violations of security policies.

11. Future Research Directions

Many approaches have faced some limitation in maintaining intrusion detection system. So some future development is needed to improve the IDS features. Firewall isolation includes by a firewall or router to mass the IP address that transfer the malicious information. Attack would embrace the tricking appropriate addresses in order to shield the hacker's paths. This means that this is not only avoiding the attacks, but also rejecting facility to a flawlessly valid user. These process shows that the hardware based system intrusion detection system have not realized proper. IPS overcomes the difficulties tackled by systems that have implemented by IDS, when the process is done correctly.

As a future process introduce a correlation of act desires for numerous network extents in a network. The process are done by data processing cycle is a comparative display of the quantity of effort vital. For this purpose the data with the supply of floating and integer point instruction are needed. To have more future application, in count to computation purpose, we examine the influence necessities by the fixed ARM9 handling policy. Furthermore work is also being done to perfect sample runs on huge circulated networking test It does not reject the use of outdated methods, such as packet analysis, which used to provide added aspects to network intrusion detection systems in a system. And also offered numerous states of attacks focused worldwide beside the network or beside specific sectors, concurrently happening with altered attacks on dissimilar sectors. In each state, some procedure of reaction was detected, even when occurrence was not focused at the Specific service.

12. Conclusion

Intrusion detection system detects malicious attacks and reports to the administrator. Actual intrusion detection and administration schemes are critical mechanisms of replicated structure as they are in the lead of the combat beside cyber-terrorism[30]. In this, we offered a context for Distributed Intrusion Detection Systems by some soft computing standards. Intrusion detection systems are planned for a system location which will develop gradually significant as the quantity and size of local area networks rise. Then model has established the feasibility of disseminated style in resolving the system-user identification[31]. We also established the status of feature decrease to typical insubstantial IDS. Finally, we suggest a hybrid style relating collective and improper classifiers for intrusion for detection[32,33]. The first security level of intrusion detection is to exercise an intrusion detection system using an eminent traditional approach with the benefits of the above approaches[34,35]. The second level of intrusion system detection is to state efficient security policies, in which the securities are based on the responsibilities. The third level of security policy is to define a security working through a device that relates the information[35]. More data mining methods are to be examined for characteristic decrease and improve the presentation of other soft computing patterns. With the collective events of cyber process[36,37], construction an active intrusion detection system with a good correctness and actual presentation are vital. Further data mining systems must be examined and productivity should be estimated as intrusion detection prototypes.

13. References

1. Modi CN, Patel DR, Patel A, Rajarajan M. Integrating signature apriori based Network Intrusion Detection System (NIDS) in cloud computing. Procedia Technology. 2012; 6:905–12.
2. Wang SS, Yan K-Q, Wang S-C, Liu C-W. An integrated intrusion detection system for cluster-based wireless sensor networks. Expert Systems with Applications. 2011; 38(12):15234–43.
3. Chung CJ, Khatkar P, Xing T, Lee J. NICE network intrusion detection and countermeasure selection in virtual network system. IEEE Transactions on Dependable and Secure Computing. 2013; 10(4):198–11.
4. Feng W, Zhang Q, Hu G, Huang JX. Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems. 2014; 37:127–40.
5. Amudhavel J, et al. An robust recursive ant colony optimization strategy in VANET for accident avoidance (RACO-VANET). International Conference on Circuit,

Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–6.
6. Amudhavel J, et al. A krill herd optimization based fault tolerance strategy in MANETs for dynamic mobility. International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–7.
7. Amudhavel J, Prabu U, Dhavachelvan P, Moganarangan N, Ravishankar V, Baskaran R. Non-homogeneous hidden Markov model approach for load balancing in web server farms (NH2M2-WSF). Global Conference on Communication Technologies; Thuckalay. 2015. p. 843–5.
8. Elhag S, Fernández A, Bawakid A, Alshomrani S, Herrera F. On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. Expert Systems with Applications. 2014; 42(1):193–202.
9. Mamalakis G, Diou C, Symeonidis AL,Georgiadis L. Of daemons and men: A file system approach towards intrusion detection. Applied Soft Computing. 2014; 25:1–14.
10. Moraes F, Abdelouahab Z, Lopes D, Oliveira E, Teixeira C, Labidi S, Teles A. Advances in self-security of agent-based intrusion detection systems. Emerging Trends in ICT Security; 2014. p. 153–71.
11. Shen X J, Liu L, Zha Z-J, Gu P-Y, Jiang Z-Q, Chen J-M, Panneerselvam J. Achieving dynamic load balancing through mobile agents in small world P2P networks. Computer Networks. 2014; 75(Part A):134–48.
12. Xia J, Luo B. A novel intrusion detection system based on feature generation with visualization strategy. Expert Systems with Applications. 2014; 41(9):4139–47.
13. Idowu RK, Maroosi A, Muniyandi RC, Othman ZA. An application of membrane computing to anomaly-based intrusion detection system. The Procedia Technology. 2013; 11:585–92.
14. Basabaa A, Sheltami T, Shakshuki E. Implementation of A3ACKs intrusion detection system under various mobility speeds. Procedia Computer Science. 2014; 32:571–8.
15. Abraham A, Jain R, Thomas J, Han SY. D-SCIDS: Distributed soft computing intrusion detection system. Journal of Network and Computer Applications. 2007; 30(1):81–98.
16. McEachen JC, Kah CW. An analysis of distributed sensor data aggregation for network intrusion detection. Microprocessors and Microsystems. 2007; 31(4):263–72.
17. Cabrera JBD, Gutierrez C, Mehra RK. Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks. Information Fusion. 2008; 9(1):96–119.
18. Lauf AP, Peters RA, Robinson WH. A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. Ad Hoc Networks. 2010; 8(3):253–66.
19. Meng Y, Li W, Kwok L-F. Towards adaptive character frequency-based exclusive signature matching scheme and its applications in distributed intrusion detection. Computer Networks. 2013; 57(17):3630–40.
20. Wang Y, Behera SR, Wong J, Helmer G, Honavar V, Miller L, Lutz R, Slagell M. Towards the automatic generation of mobile agents for distributed intrusion detection system. The Journal of Systems and Software. 2006; 79(1):1–14.
21. Huang W, An Y, DuSch W. A multi-agent-based distributed intrusion detection system. Advanced Computer Theory and Engineering, ICACTE; 2010.
22. Seresht NA, Azmi R. MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach. Engineering Applications of Artificial Intelligence. 2014; 35:286–98.
23. Hubballi N, Suryanarayanan V. False alarm minimization techniques in signature-based intrusion detection systems. Computer Communications. 2014; 49:1–17.
24. Peng T, Leckie C, Ramamohanarao K. Information sharing for distributed intrusion detection systems. Journal of Network and Computer Applications. 2007; 30(3):877–99.
25. Vacca JR, Syngress B. Intrusion prevention and detection systems. Managing Information Security. 2013.
26. Shamshirband S, Anuar NB, Kiah MLM, Patel A. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence. 2013; 26(9):2105–127.
27. Veetil S, Gao Q. Real-time network intrusion detection using hadoop-based bayesian classifier. Emerging Trends in ICT Security; 2014. p. 1–3.
28. Patel A, Taghavi M, Bakhtiyari K, Junior JC. An intrusion detection and prevention system in cloud computing. A systematic review. Journal of Network and Computer Applications. 2013; 36(1):25–41.
29. Corona I, Giacinto G, Roli F. Adversarial attacks against intrusion detection systems, Taxonomy, solutions and open issues. Information Sciences. 2013; 239:201–25.
30. Koc L, Mazzuchi TA, Sarkani S. A network intrusion detection system based on a hidden naive bayes multiclass classifier. Expert Systems with Applications. 2012; 39(18):13492–500.
31. Gowrison G, Ramar K, Muneeswaran K, Revathi T. Minimal complexity attack classification intrusion detection system. Applied Soft Computing. 2013; 13(2):921–7.
32. Meng W, Li W, Kwok L-F, EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. Computers and Security. 2014; 43:189–204.
33. Wang W, Guyet T, Quiniou R, Cordier M-O, Masseglia F, Zhang X. Autonomic intrusion detection. Adaptively detecting anomalies over unlabeled audit data streams in computer networks. Knowledge-Based Systems. 2014; 70:103–17.
34. Horng S-J, Su M-Y, Chen Y-H, Kao T-W, Chen R-J, Lai J-L, Perkasa C-D, et al. A novel intrusion detection

system based on hierarchical clustering and support vector machines. Expert Systems with Applications. 2011; 38(1):306–13.

35. Costa KAP, Pereira LAM, Nakamura RYM, Pereira CR, Papa JP, Falcao AX. A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks. Information Sciences. 2015; 294:95–108.
36. Uddin M, Alsaqour R, Abdelhaq R. Intrusion Detection System to Detect DDoS Attack in Gnutella hybrid P2P network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.
37. Javidi MM, Rafsanjani MK, Hashemi S, Sohrabi M. An overview of anomaly based database intrusion detection systems. Indian Journal of Science and Technology. 2012 Oct; 5(10):3550–9.