International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

High Performance Network Intrusion Detection System

Anita Bai, R. Delshi Howsalya Devi, R. Madana Mohana

Abstract*: In this paper, we present intrusion detection system for finding the variant types of attacks in the network. It is the way to enhance the functionality in the network by reducing the chances of risks. ICMP protocol and AES encryption algorithm are used to report the error messages and manage the information being sent from source to destination. If there is any malicious activity occurred in the network, the user will be alerted of it by specifying them the type of malicious activity. As a result it reduces the chances of intrusions and contacting multiple resources for resolving single issue.

Keywords*: AES encryption, ICMP protocol, Intrusion detection systems, Network security.

I. INTRODUCTION

Currently information technology is growing and increasing rapidly which generates an enormous amount of data is helpful into our daily life. This data requires data processing, its operations and maintenance. During these process malicious attacks and affects the public and personal data in computer systems. To protect the data from attackers we can use Intrusion Detection System. Intrusion Detection System (IDS) is a system or software application which is used to monitor the network (suspicious activities). It report error, if any malicious activity found in the network [1, 3]. IDS work with the snort open-source NIDS that handles the underutilized computational power of modern graphics. IDS reduce the pattern matching operations cost from the CPU which increases overall processing throughput. Therefore we can analyze and evaluate various IDS tools which will help for high speed networks. Intrusion Detection System (IDS) is used to provide network security and alert system administrator when suspicious attempts or access found in the network. Action of IDS is depending on the situations sometimes IDS can simply alert the user/administrator or else it possibly will be set up to block specific traffic or automatically respond in some way [4, 16]. There are available two primary methods for monitoring: signature-based and anomaly-based. a) Signature-based detection depends on comparison of traffic with the database having signatures of known attack methods [8]. b) Anomaly-based detection analyzes current network traffic with a known-good baseline to look for anything out of the ordinary [14, 10]. Many data mining algorithms such as Frequent item set mining [11], High utility item set mining [12] and Similarity analysis [13, 22] can be used to identify any type of attack which occurred frequently in the network.

Firewall is a network security hardware or software system that is placed between two or more computer networks to monitors and controls committed attacks over the network traffic [7, 17]. From literature we can observe firewalls are not capable to secure a network fully because anytime attacks can be acted from outside the network. In this situation intrusions detection systems (IDSs) can be very useful to identify and stop attacks, recover from them with the minimum loss or analyze the security problems so that it will be not repeated in future [9,15,18]. IDS help to detect suspicious attacks and misuses of the system by collecting information from a computer or over a computer network.

We can use IDS as a NIDS (network-based intrusion detection) with some strategies on the network. It can be installed on each individual system as a HIDS (host-based intrusion detection) or it can examine all network traffic which investigates traffic from and to particular device only.

II. TYPES OF ATTACKS

A. IP Spoofing

IP (Internet Protocol) forms the third layer of the ISO model. It is the network protocol which is used for the transmission of messages over the internet. Every email message sent has details in the message header of the IP address of the sender (source address). Hackers and scammers alter the header details to mask their true identity by editing the source address. The emails then appear to have been transmitted by a trusted source. There are two types of IP spoofing [5] as follows:

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Dr. Anita Bai*, Associate Professor, Computer Science & Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telangana. anitabai@biet.ac.in, anitaahirwarnitr@gmail.com
Dr. R. Delshi Howsalya Devi, Associate Professor, Computer Science & Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telangana. delshi@biet.ac.in, delshi@rocketmail.com
Dr. R. Madana Mohana, Professor, Computer Science & Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telangana. madanmohanr@biet.ac.in

- Man In the Middle Attacks: As the name suggests, communication between the original sender of the message and the desired recipient is intercepted. The content of the message is then modified without the knowledge of either party. The attacker feeds the packet with his own message. The victim is deceived into thinking the contents of the message are authentic.
- Denial of Service (DoS) Attacks: In this practice, the message packet between the sender and the recipient is intercepted and the source address is spoofed. The connection is literally hijacked.

B. Bandwidth Spoofing:

Spoofing means imitate or trick someone. Bandwidth Spoofing is a one of the attack in which disable the someone else's infrastructure by producing a traffic overload. The bandwidth attack result may vary in the protocol which can be use to mount the attack [19, 20].

C. Packet Spoofing:

Over the computer network when any data is transferred, it broken down into chunks with various pre-defined tags such as preambles, MAC addresses (source and destination) and frame checksum code at the senders side, termed data packets and it will be reassembled at receiver's node in original format. A segment, a block, a cell or datagram is the chunk/pieces of communication across a computer network. Packet sniffing is the process of monitoring the data packet over the computer network. It is same as wire tapping to a telephone network. It is generally used by governments, ISPs and advertisers. It is also used to collect illegal information about the network by crackers and hackers.

III. PROPOSED SYSTEM

In this paper, we propose a technique for securing nodes by using knowledge-based ids (kb-ids) in a cluster based wireless sensor networks. Knowledge-based ids are used to keep record of various behaviors of nodes over the network. The knowledge base possibly will be huge in the size and require extensive computation. Therefore we have to store it on the base station. Cluster-based intrusion detection mechanism is a good choice for smart wireless sensor networks. The CHS uses inference engine to monitor the activities in the base station. This can observe the network traffic and its nodes behavior, and alert errors by sensing possible attacks over the nodes with the help of security context sensors. Furthermore, inference engines forwarded the error message to the base station for next processing. Finally, all the provided suspicious data will be keep, analyse, compute and conclude by the base station.

A. System Design And Development

Fig. 1 is showing system architecture of IDS. IDS include service provider, router, attacker and IDS manager to detect attack over the network.

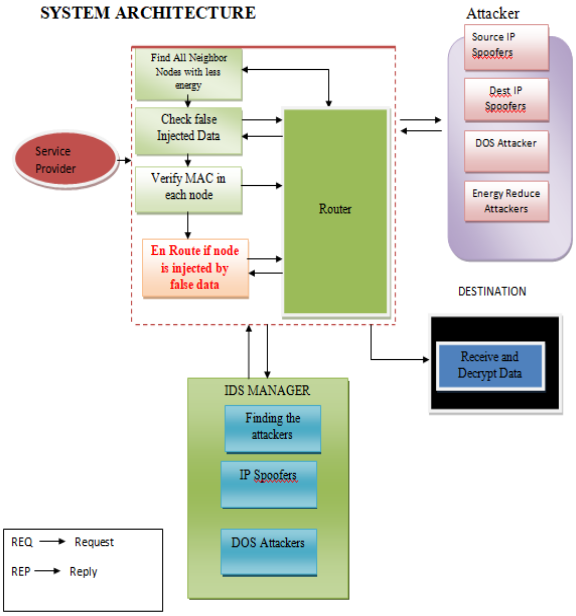

Fig.1. System Architecture of IDS

B. Modules

- **Service provider**

The main task of service provider is to look through the data file and the router nodes initialization. To provide the security to all service providers always encrypts the data file and then send it to all the receivers (A, B, C, D…). The responsibility of service provider is to send their data file to router and then router will send the data files to the associated receiver by selected smallest distance path [2].

- **Router**

Router provides data storage services by managing multiple nodes include N number of nodes (n1, n2, n3, n4, n5…). Router service provider can monitor the details of nodes and their routing paths. Role of service provider is to send their data files to the router then router will choose least distance path and then it can send the data files to the associated receiver. In a node, if any attacker is to be found then IDS manager will activate and send message to router. Router can connect with files to another node which is send to the particular receiver.

- **IDS Manager**

IDS Manager is capable to detect introducers and can keep details of all introducers. If any type of attacker such as all Spoofers like DOS Attacker, source and destination is found in the router then attacker details will send to IDS manager. The main role of IDS Manager is to detect the attacker type i. e active attacker or passive attacker and response send to the router. Additionally, IDS Manager is capable to see the attacker's details with their fields such as attacked node name, attacker type, attack time and date.

- **Receiver (End User)**

The main work of receiver is to receive the data file from the router. The service provider sends data files to the router and then router accept the data files and forwarded to their associated receivers

(A, B, C, D, E and F). Decrypted format are used to transfer theses data files without alter the file contents. Inside the network, users can receive particular data files [7, 21].

- **Attacker**

Generally two types of attackers are available: Active and Passive. a) Active attacker is a attacker which is allow to inject malicious data to the corresponding node and, b) Passive attacker is a attacker which can change the destination IP of the particular node. Inside router we can view attacked nodes details after attacker attack.

IV. EXPERIMENTAL SETUP AND RESULTS

A. Experimental Setup: We run on Windows 7, Intel i3 using Java programming.

B. Experimental Studies: The main purpose of testing is to discover abnormal errors. In the testing process we can try to discover every weakness or conceivable fault in a work product.

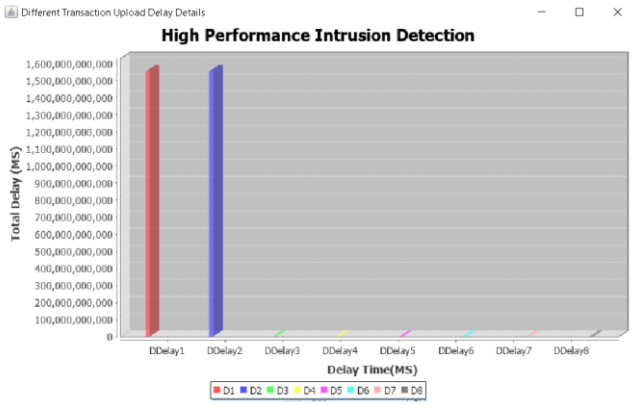

Fig. 2. Time Delay

When there is a time delay while sending the information from sender to receiver in the case of attack then it is intimated in this graph by these lines shown in Fig. 2. When we run the NODE A destination the initial screen as shown in Fig. 3 and when we run the Router the initial screen as shown in Fig. 4. When we run the attacks the initial screen as shown in Fig. 5. When we browse a file in the sender as shown in Fig. 6.

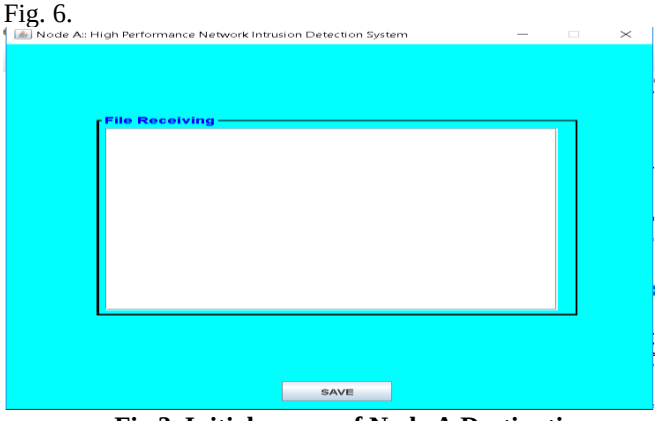

Fig.3. Initial screen of Node A Destination

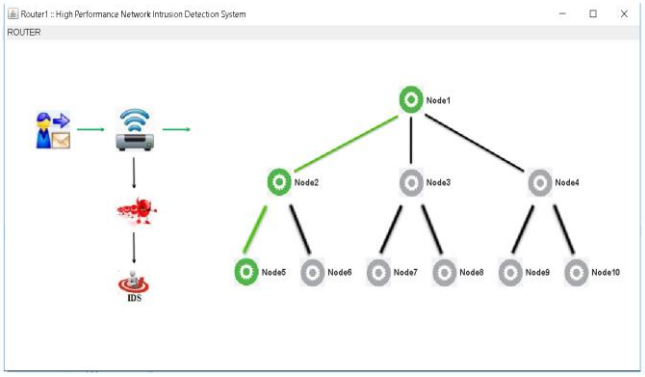

Fig. 4. Router Initial Screen

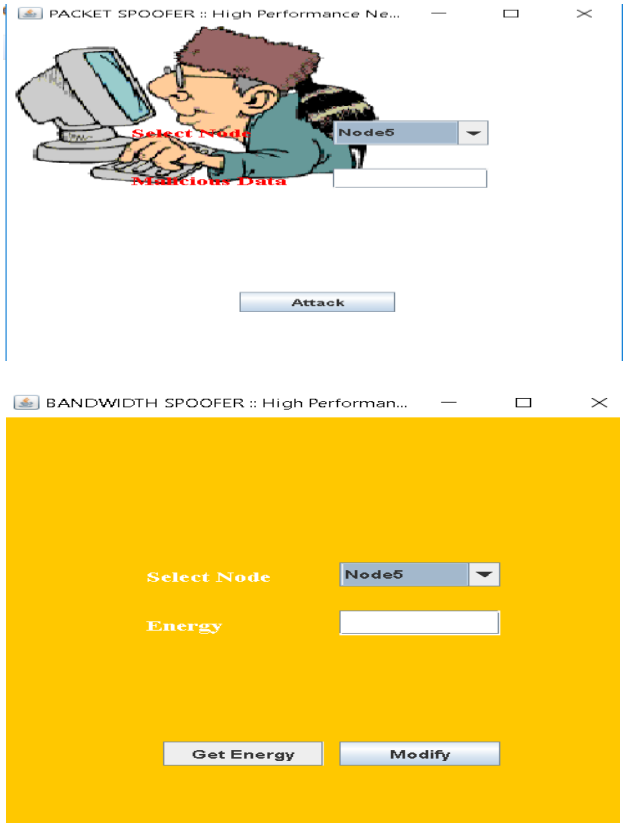

Fig. 5. Initial Screens of Attacks

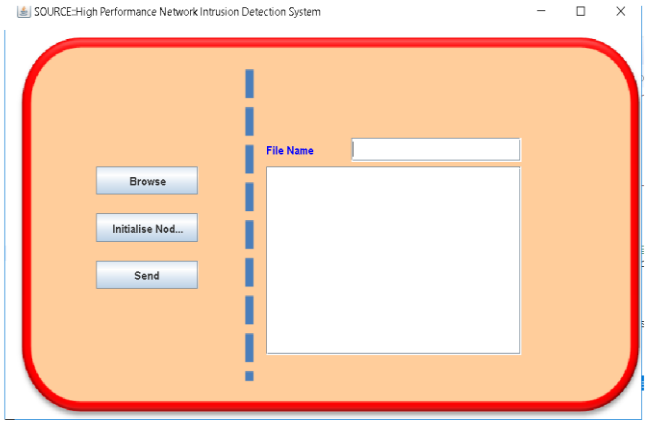

Fig. 6. Service Provider Screen when file is browsed.

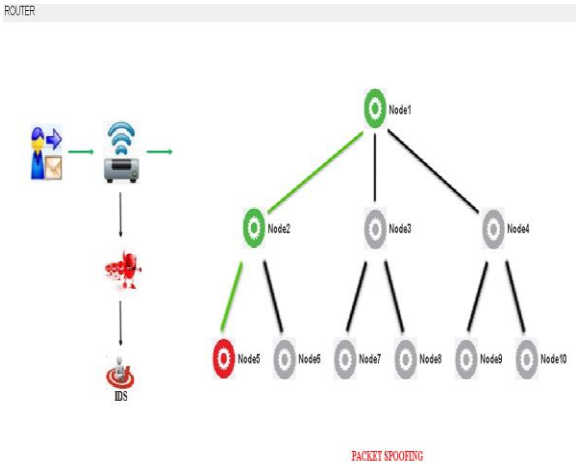

Fig. 7. Screenshot of the router without attack

When we send the file from source to destination and there is no attack in the network then this is the result at the router. No attack indicates nodes in green colour shown in Fig. 7.

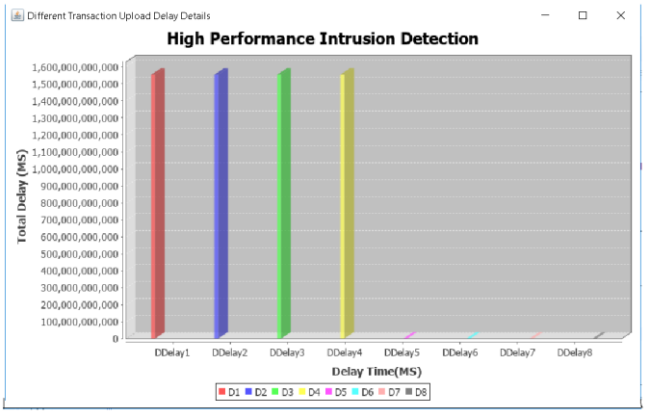

Fig.8 Results Screen for IDS

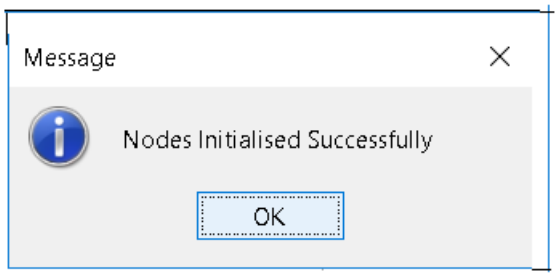

Fig. 9. Screenshots for the file initialized successfully.

Total delay details for IDS are showing in Fig. 8. When we browse a file to send from source to destination then once the nodes are initialised in the sender, we get this popup message indicating the nodes are initialised successfully is showing in Fig. 9.

C. Result Analysis

To show the effectiveness and efficiency of our approach we are showing comparison of the proposed system with existing methods in Table-I.

V. CONCLUSIONS AND FUTURE SCOPE

In this paper, the load is distributed among all the nodes equally to enhance the computing efficiency and there on calculating the time delay between the source to destination to send the information in a network. The graph representing the time delay can clearly elucidate the delay between them. The malicious activity occurred is identified by specifying the type of attack and letting the client to resolve the issue sooner than before. The enhancement can be imparting the dynamic routing system.

In future we are planning to add advanced technologies for enhancements. As part of technical build-up many components of the networking system will be generic in nature so that further we can use with this.

REFERENCES

1. A. Mehmood, Akbar Khanan & Muhammad Muneer Umar, “Secure Knowledge and Cluster-based Intrusion Detection Mechanism for Smart Wireless Sensor Networks,” IEEE Access Volume: 6, 5688-5694, 2018.
2. A. Wahid and P. Kumar, ‘‘A survey on attacks, challenges and security mechanisms in wireless sensor network,’’ Int. J. Innov. Res. Sci. Technol.,vol. 1, no. 8, pp. 189–196, 2015.
3. https://www.sih.gov.in/
4. A. Alam and D. Eyers, ‘‘Securing WSN update from intrusion using timesignature of over the air update protocol,’’ in Proc. 13th Australasian Symp. Parallel Distrib. Comput. (AusPDC), pp. 107–110, 2015.
5. Mohammed Hassan Ali, Bahaa Abbas Dawood Al Mohammed, Alyani Ismail, “A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization,” IEEE Access Volume:6,20255-20261.
6. A. Mehmood, A. Khanan, A. H. H. M. Mohamed, and H. Song, ‘‘ANTSC: An intelligent Naïve Bayesian probabilistic estimation practice for traffic flow to form stable clustering in VANET,’’ IEEE Access, to be published,doi: 10.1109/ACCESS.2017.2732727.
7. A. Mehmood, S. Khan, B. Shams, and J. Lloret, ‘‘Energy-efficient multi-level and distance-aware clustering mechanism for WSNs,’’ Int. J. Commun. Syst., vol. 28, no. 5, pp. 972–989, 2015.
8. I. Butun, S. D. Morgera, and R. Sankar, ‘‘A survey of intrusion detection systems in wireless sensor networks,’’ IEEE Commun. Surveys Tuts.,vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.
9. https://searchsecurity.techtarget.com/definition/intrusion-detection-system
10. A. Mehmood, J. Lloret, and S. Sendra, ‘‘A secure and low-energy zone based wireless sensor networks routing protocol for pollution monitoring,’’ Wireless Commun. Mobile Comput., vol. 16, no. 17, pp. 2869–2883, 2016.
11. A. Bai, P.S. Deshpande, and M. Dhabu, “Selective database projections based approach for mining high-utility itemsets.” *IEEE Access, vol.* 6, pp.14389-14409, 2018.
12. A. Bai, M. Dhabu, V. Jagtap, and P. S. Deshpande, “An efficient approach based on selective partitioning for maximal frequent itemsets mining.” *Sādhanā, vol.* 44, no. 8, pp. 183, 2019.
13. A. Bai, S. Hira, and P. S. Deshpande, “Recurrence based similarity identification of climate data”, *Discrete Dynamics in Nature and Society*, 2017.
14. A. F. Serpella, X. Ferrada, R. Howard, and L. Rubio, ‘‘Risk management in construction projects: A knowledge-based approach,’’ Proc.-Soc. Behavioral Sci., vol. 119, pp. 653–662, Mar. 2014.
15. https://www.techopedia.com/definition/3988/intrusion-detection-system-ids
16. https://en.wikipedia.org/wiki/Intrusion_detection_system
17. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids
18. https://www.elprocus.com/basic-intrusion-detection-system/
19. https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
20. http://www.rroij.com/open-access/importance-of-intrusion-detection-system-withits-different-approaches.php?aid=41367
21. www.stackoverflow.com
22. Anita Bai, Swati Hira, P. S. Deshpande, “An Application of Factor Analysis in the Evaluation of Country Economic Rank”, Procedia Computer Science, Elsevier, vol. 54, pp. 311-317, 2015

AUTHORS PROFILE

Dr. Anita Bai, received the Ph.D. from Visvesvaraya National Institute of Technology, Nagpur, India and the M.Tech. degree from National Institute of Technology, Rourkela, India. She is currently an Associate professor with the Department of Computer Science and Engineering at Bharat Institute of Engineering and Technology, Hyderabad, Telangana, India. She has co-authored a number of research articles in various journals, conferences, and book chapters. She is associated with IAENG, IEEE Access, Sadhana, and International Journal of Recent Scientific Research. She has published 2 patents and 1 patent were filed. She is guiding 2 M.Tech scholars registered at JNTUH, Hyderabad, India. Her research interests include data mining, big data analytics, soft computing and machine learning.

Prof. Dr. R. Delshi Howsalya Devi, received her BE (distinction) in Computer Science and Engineering from the Madurai Kamaraj University, Madurai, in 2004, ME in Computer Science and Engineering from the Anna University, Chennai, in 2008 and PhD in Information and Communication Engineering from the Anna University Chennai in 2018. She is an Associate Professor at the Department of Computer Science and Engineering, Bharat Institute of Engineering and Technology, Hyderabad, Telungana. She has 14 years of teaching experience and has approximately 29 conference publications and 18 international journal publications. She has published 5 National Patents. She is guiding 2 M.Tech scholars registered at JNTUH, Hyderabad, India. She is associated with IEEE access Journal, Journal of Supercomputing, Springer, Journal of Ambient Intelligence and Humanized Computing, Springer, Acta Scientific Pharmacology and Reviewer for 2020 3rd International Conference on Applied Mathematics, Modeling Shanghai. She was acted as a technical committee member in many reputed conferences so far. She was received a National Award titled "Young Educator and Research Scholar" by National Foundation for Entrepreneurship Development and she was acted as panel judge in hackathon. Her research interests include Data Mining, Image Processing, Outlier Mining, Cloud Computing, Big data Analytics and Biomedical data analysis.

Dr. R. Madana Mohana, is currently working as Professor in the Department of the Computer Science and Engineering at Bharat Institute of Engineering and Technology, Ibrahimpatnam - 501 510, Hyderabad, Telangana. Received Ph.D in Computer Science & Engineering, Sri Venkateswara University, Tirupati. His research interests include Machine Learning, Data Mining, Bigdata, Information Retrieval and Computational Intelligence. He is a Life Member of ISTE and Member of CSI & ACM. He published 34 papers in journals and conferences of repute, 8 patents were filed and 3 patents are published.

Table-I: Comparison of the proposed system with existing methods

Input data->File type	Results of Existing Method	Proposed Method Results	Remarks
FILE→.java file	The attack can be identified but the type of attack is unknown.	The attack with the node blocked, type of attack is known.	Enhancement of Existing Method.
FILE→.java file	The nodes information, time delay, digital signature and router details all are not known in single system.	All are consolidated into one place and the nodes information, time delay, digital signatures and router details are known	Consolidation of Existing Methods.