Intruder Detection Analysis using Hybrid Algorithm

Abstract：**In Block Chain system Security issues are most basic issues of wireless networks. Different types of attack such as Intrusion exist in a network which may corrupt the data in a communication. Where Intrusion in an information system is the activity which violates the security policy of the system. Intrusion detection is the process used to identify intrusions. Intrusion detection system is device or software application that monitors network and/or system activities for malicious activity or polices violations and reports to the management system. In this paper we are going to propose the intrusion detection by using simulation and clustering. We have used various response techniques which includes IDPS.**

KEYWORDS: Intrusion Detection, BPN, Blockchain Computing, WSN

I

I. INTRODUCTION

The Intrusions used in system to activities that violate the security policy of the system, and intrusion detection used for identify intrusions. An intrusion detection system (IDS) is a device or software application that monitors network and system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion prevention systems are mainly focused on prevention possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

II. Research Methodology

IDS may be classified into Network-based IDSs and host based IDSs according to the sources of the audit information used by each IDS. There are two main types of IDS:

A. Network intrusion detection system (NIDS)

NIDS identifies intrusions by examining network traffic and monitors multiple hosts. This systems gain access to network Transmission by collaborative a network hub, network switch configured for port mirroring, or network tap. In a NIDS, has located at main points in the network to be monitored, also in the demilitarized zone and at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic. An example of a NIDS is Snort.

B. Host-based intrusion detection system (HIDS)

It has an program on a host that identifies intrusions by analyzing system data, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities and state. In a HIDS, usually consist of a program application. An example of a HIDS is OSSEC. Intrusion detection systems will detected specific type using programming.

I. INTRUSION TECHNIQUES

Intrusion detection systems must be capable of differentiating normal and abnormal activities, to discover malicious attempts in time. Many behavior patterns are unpredictable and unclear (Fig. 2). In order to classify actions, intrusion detection systems take advantage of the anomaly detection approach, sometimes referred to as behavior based or attack signatures i.e. a descriptive material on known abnormal behavior (signature detection), also called knowledge based

A. *Anomaly detection*

Normal behavior patterns are useful in predicting both user and system behavior. Anomaly detectors construct profiles that represent normal usage and then use current behavior data to detect a possible mismatch between profiles and recognize possible attack attempts. In order to match event profiles, the system is required to produce initial user profiles to

train the system with regard to legitimate user behaviors. An inappropriate profile will be able to detect all possible intrusive activities. Furthermore, there is an obvious need for profile updating and system training which is a difficult and time-consuming task. Given a set of normal behavior profiles, everything that does not match the stored profile is considered to be a suspicious action. Hence, these systems are characterized by very high detection efficiency (they are able to recognize many attacks that are new to the system), but their tendency to generate false alarms is generally a problem.

Advantages of this anomaly detection method for detection of novel attacks as intrusions; and anomalies are recognized without getting inside their characteristics; less dependence of IDSs on operating environment as compared with attack signature-based systems ability to detect abuse of user privileges.

B. *Misbehavior signatures — signature detection*

Systems possessing information on abnormal, unsafe behavior (attack signature-based systems) are often used in real-time intrusion detection systems because of their low computational complexity.

The misbehavior signatures fall into two categories:

- Signatures Attack–describe action type that may pose a security threat.
- Strings Selected text– suspicious action signatures to match text strings.

Any action that is not proper will be prohibited is allowed. Typically, they do not achieve completeness and are not immune to novel attacks. There are two main approaches with signature detection:

- Verification of the pathology of lower layer packets— many types of attacks exploit flaws in IP, TCP, UDP or ICMP packets. With a very simple verification of flags set on specific packets it is possible to determine whether a packet is legitimate or not. Difficulties may be encountered with possible packet fragmentation and the need for re-assembly.
- Verification of application layer protocols — many types of attacks exploit programming flaws, for example, out-of-band data sent to an established network connection. In order to effectively detect such attacks, the IDS must have implemented many application layer protocols. The signature detection methods have the following advantages: very low false alarm rate, simple algorithms, and easy creation of attack signature databases, easy implementation and typically minimal system resource usage. Commercially offered IDS products often use the signature detection method for two reasons. Firstly, it is easier for a given signature to be associated with a known attack abstraction and to assign a name to an attack. Secondly, the attack signature database must be updated regularly (by adding signatures of newly discovered attacks and exploits), which may create a fairly good source of income for vendors of IDS tools. A database update is at the same time a less cumbersome task than that associated with the change of typical user behavior profiles. In the latter case, a temporary closing down of the system may be required, what cannot be tolerated on certain applications.

So the proposed system incorporates a technique that performs data authentication to detect attacker. Thus system built is electing another aggregator node. Hence authenticated data is securely received at base station.

Security research challenges and open questions which may be future research directions to enable secure data aggregation in WSNs. Despite the research efforts to improve this issue, there is no ideal scheme that can meet the security requirements for data aggregation and resolve all the problems caused by the special characteristics of WSNs. Therefore, for WSNs security researchers to focus on the challenges we have set out. Networks are typically deployed in hostile environments and in which privacy and data integrity are widely desired. Because of their design, wireless sensors can be easily captured. Also, nodes that perform the aggregation function are most attractive to attackers. Therefore, in order to deal with these security threats, the research on data aggregation security is essential.

III. Implementation

- Generation of Network: Generate network of sensor nodes. Those nodes are connected through the edges.
- Formation of Cluster: The clustering process is performed in network system; the mobile nodes are divided into group of clusters. Number of clusters is generated in the sensor network.
- Selection of Cluster Head: Cluster head is selected from clusters. Aggregator selection is done by using parameters like highest remaining energy of the nodes. This step is performed twice, after initial formation of clusters and for

selection of new aggregator on detecting attack on old aggregator.

- Iterative Filtering: The new IF algorithm is used for detection compromised node in sensing network. This iteratively checks the readings and assigns weights to the node.
- Detection of Compromised Node: Compromised nodes are detected by comparing the weights to the threshold. The node with less weight is considered as the compromised node. It works for both the cluster members and aggregation too.
- New aggregation node selection with hashing: Base station can detect the attack on data aggregation node. In this concept of hashing is used. Here, all cluster members send the data to data aggregation node along with hash of their sensed data. Next aggregation nodes collect and aggregate the data and hash from all nodes and forward it to the base station. On receiving the data with hash, base station again generate the hash of the received data. If the hash not matched, then the base station assume that the attack is occur on aggregation node and at the same time base station discard that data and aggregation node. Also assign new data aggregation node based on maximum energy and distance to neighboring node and base station.

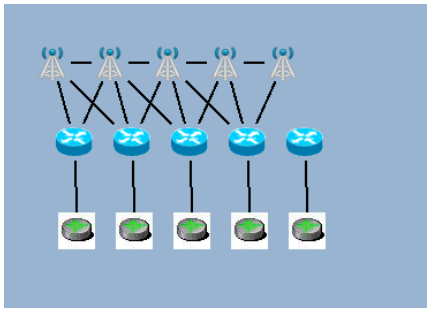

Figure 1. Generation of Network with sensor nodes.

1) Network generation: This will periodically send handshaking messages to their tower to ensure that they are functional, and also report changes to the one-hop neighbors. Missing messages can be used to detect the failure of these. Once a failure is detected in the neighborhood, the one-hop neighbors of the failed the would determine the impact

.

2) Capacity identification: limits of data transmission of each tower nodes in the smallest block to reduce the recovery overhead. The smallest block is the one with the least number of nodes and would be identified by finding the reachable set of nodes for every direct neighbor of the ailed node and then picking the set with the fewest nodes. Since a critical node will be on the sho path of two nodes in separate blocks, the set of reachable nodes can be identified. In other words, two nodes will be connected only if they are in the same block.

3) Changing the path: If tower is the neighbor of the tower that belongs to the smallest block, it is considered the to replace the fail path. Since it is considered the gateway of the failed path (and the rest of the network), we refer to it as "parent." A node is a "child" if it is two hops away from the failed node, "grandchild" if three hops away from the failed node, and so on.

4) The foregoing discussion has assumed that system are aware of the network topology and can assess the impact of the failure and uniquely identify which node should replace the failed the. If every tower in the network is communicating with all the other nodes, it would be possible to fully populate the routing table and for the individual nodes to reach consistent decisions without centralized coordination.

Vitality Efficiency: By the data-aggregation plot, we can build the usefulness of the wireless sensor network. In which each sensor hubs ought to have spent a similar measure of vitality in each datum assembling round. A data aggregation conspire is vitality proficient in the event that it augments the usefulness of the network. Network lifetime, data exactness, and inertness are a portion of the critical execution measures of data-aggregation calculations. The meanings of these measures are exceptionally subject to the coveted application. Network lifetime: The network lifetime is characterizing the quantity of data combination rounds. Till the predefined. level of the aggregate hubs passes on and the rate rely upon the application .If we discuss some application, simultaneously working of the all the hubs is vital thus the lifetime of the network is number of round until the main hubs which enhances

the vitality proficiency of hubs and improve the lifetime of entire network. Idleness: Latency is assess data of time defer encounters by system, implies data send by sensor hubs and got by base station (sink).basically postpone associated with data transmission, steering and data aggregation. Correspondence overhead: It assesses the correspondence unpredictability of the network combination calculation. Data precision: It verifies the proportion of aggregate

MESSAGE PACKET SECURITY ALGORTHIM

The DES with MD5 improved security against power analysis attacks. The proposed designs use Boolean masking, a previously introduced technique to protect smart card implementations from these attacks. Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement.DES encrypts data in 64-bit and it is a symmetric algorithm. The key length is 56-bits. In cryptography, the **Data Encryption Algorithm** (**3DES**) is a block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. As a block cipher, it is also symmetric. The algorithm was intended as a replacement for the Data Encryption Standard (DES). DES is a minor revision of an earlier cipher, Proposed Encryption Standard (PES); 3DES was originally called Improved PES (IPES). Due to its strength against cryptanalytic attacks and due to its inclusion in

several popular cryptographic packages, 3DES is widely used. Combine with **AES algorithm** is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard

Figure 2. Detection of Compromised Node.

We can classify data aggregation security solutions into two categories namely the hop-by-hop solutions and end-toend solutions. In the first category, cryptography is applied hop-by-hop, which the security services are checked in each step, the intermediate nodes decrypt each received message and calculate the aggregate before encrypt it. This method allows a simple implementation of aggregate functions, and it imposes no limits on their nature (sum, average, variance, maximum, minimum, etc.) and two types of encryption can be used. Also, these solutions incur significant delay and this is due to the encryption/decryption effort performed by the intermediate nodes. These problems were solved by end-to-end solutions based on a special property of encryption algorithms called privacy homomorphic encryption.

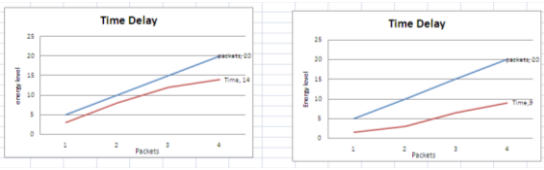

Figure 3. Packet Filtering Ratio

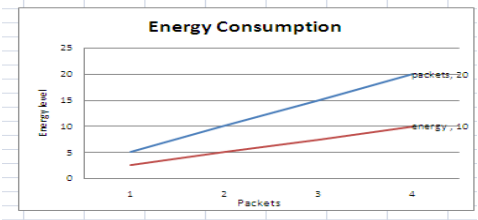

Figure 4. Packet Energy Ratio

This is used for the packet transmission and load balancing for the network system. In this System the number of path link calculate for through which the packet distribution is generated And load balancing is maintain. Through which the network is balance.

IV. Conclusions

Block chain technology is an emerging solution for decentralized transactions and data management without the need of a trusted third party. It is an open and distributed ledger, enabling the recording of transactions among various parties in a verifiable way. To date, blockchains have been studied in several domains like healthcare and supply chain management, but there has been little work investigating its potential application in the field of intrusion detection. Motivated by this observation, our work mainly discusses the applicability of blockchain technology to mitigate the challenges of data sharing and trust computation in a collaborative detection environment. We identify that blockchains have a potential impact on the improvement of an IDS, whereas not all IDS issues can be solved with this technology.

Reference

1. Alexopoulos, N., Vasilomanolakis, E., Ivanko, N.R., Muhlhauser, M.: Towards blockchain-based collaborative intrusion detection systems. In: Proceedings of the 12th International Conference on Critical Information Infrastructures Security, pp. 1–12 (2017).

2. Almost half of companies still can't detect IoT device breaches, reveals Gemalto study. Accessed 10 Apr 2019

3. Amazon Managed Blockchain: easily create and manage scalable blockchain networks. Accessed 10 Apr 2019

4. Badertscher, C., Gazi, P., Kiayias, A., Russell, A., Zikas, V.:Ouroboros genesis: composable proof-of-stake blockchains with dynamic availability. In: Proceedings of ACMConference on Computer and Communications Security (CCS), pp. 913–930 (2018)

5. Daian, P., Pass, R., Shi, E.: Snow white: robustly reconfigurable consensus and applications to provably secure proofs of stake. In: Financial Cryptography and Data Security (FC) (2019)

6. Duma, C., Karresand, M., Shahmehri, N., Caronni, G.: A trustaware, P2P-based overlay for intrusion detection. In: DEXA Workshop, pp. 692–697 (2006)

7. Fadlullah, Z.M., Taleb, T., Vasilakos, A.V., Guizani, M., Kato, N.: DTRAB:combating against attacks on encrypted protocols through traffic-feature analysis. IEEE/ACMTrans. Netw. **18**(4), 1234–1247 (2010)

8. Friedberg, I., Skopik, F., Settanni, G., Fiedler, R.: Combating advanced persistent threats: from network event correlation to incident detection. Comput. Secur. **48**, 35–47 (2015)

9. Fung, C.J., Baysal, O., Zhang, J., Aib, I., Boutaba, R.: Trust management for host-based collaborative intrusion detection. In: De Turck, F., Kellerer, W., Kormentzas, G. (eds.) DSOM 2008, LNCS 5273, pp. 109–122 (2008)

10. Fung, C.J., Zhu, Q., Boutaba, R., Basar, T.: Bayesian decision aggregation in collaborative intrusion detection networks. In: NOMS, pp. 349–356 (2010).

11. Wang, Y., Meng, W., Li, W., Liu, Z., Liu, Y., Xue, H.: Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems. Concurr. Comput. Pract. Exp. **31**(19), e5101 (2019)