Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# An Efficient Authentication Method for Detecting the Intrusion Using IDPS in WSN

[1]M. Kalaiselvi, [2]S. Priya
[1]M.E, (Ph.D)., Assistant Professor, [2] PG Scholar
[1, 2] Department Computer Science and Engineering, Vivekanandha College of Technology for Women, Sathinaickanpalayam, Tiruchengode, Tamilnadu, India

***Abstract:*** ***In networking, the DDOS threat is major concern which creates the severe attack between the server and users. The internet attacks' circumstance is increasing in the direction of a distributed, mutual direction. Attacks of internet drain a lot of resources; creation of the victim host cannot accept normal network requests take up a grouping of bandwidth, resulting in substantial losses of economic in network. It is not easy to identify the exact signature of attacking and Intrusion detection systems are a key module in ensuring the safety of networks and systems. Therefore, we propose a signature based Intrusion detection with the interrelation of IP address analysis. IDPS (Instruction detection and prevention system) is automatically eliminating the attacks and adopts the distributed architecture to monitor intrusion activities. Realize abnormal events processing in local nodes.This paper focused on distribution of network traffic during the data transmissions using DDOS detection scheme based on the IP address analysis. By using this proposed method, the DDOS attack will be decreased and also the reliability in data transmission is increased.***

***Keywords: DDOS attack, IP address analysis, Instruction detection and prevention system, Cluster Head artificial immune system, Multivariate correlation analysis.***

## I. INTRODUCTION

Wireless Sensor Networks have emerged as research areas with an overwhelming effect on practical application development. They permit fine grain observation of the ambient environment at an economical cost much lower than currently possible. In hostile environments where human participation may be too dangerous in sensor network which may provide a robust service. Sensor networks sensor nodes to a data repository on a server. The advances are designed to transmit data from an array of in the integration of MEMS, microprocessor and wireless communication technology have been enabled the deployment of large scale. WSN has potential to design many new applications for handling emergency, military and disaster relief operations that requires real time information for efficient coordination and planning.

Sensors are devices that produce a measurable response to a change in a physical condition like temperature, humidity, pressure etc. WSNs may consist of many different types of sensor such as seismic, magnetic, thermal, visual, infrared, and acoustic and radar capable to monitor a wide variety of ambient conditions. Through each individual sensor may have severe resource constraint in terms of energy, memory, communication and computation capabilities; large number of them may collectively monitor the physical world and process the information on the fly environment. A WSN is different from other popular wireless networks **circumstance is increasing in** like cellular network, WLAN and Bluetooth in many ways.

Compared to other wireless networks, a WSN has much more nodes in a network, distance between the neighbouring nodes is much shorter and application data rate is much lower also. Due to these characteristics, power consumption in a Sensor network will be minimized. To keep the cost of the entire sensor network down, cost of each sensor needs to be reduced. It is also important to use tiny sensor nodes. A smaller size makes it easier for a sensor to be embedded in the environment it is in. WSNs may also have a lot of redundant data since multiple sensors can sense similar information. The sensed data therefore need to be aggregated to decrease the number of transmission in the network, reducing bandwidth usage and eliminating unnecessary energy consumption in both transmission and reception.

The main characteristics of a WSN include,

- Power consumption using batteries or energy harvesting
- Ability to cope with node failure
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale deployment
- Ease of use

In a WSN, sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards a sink, which could be a gateway, base station, storage node, or querying user.

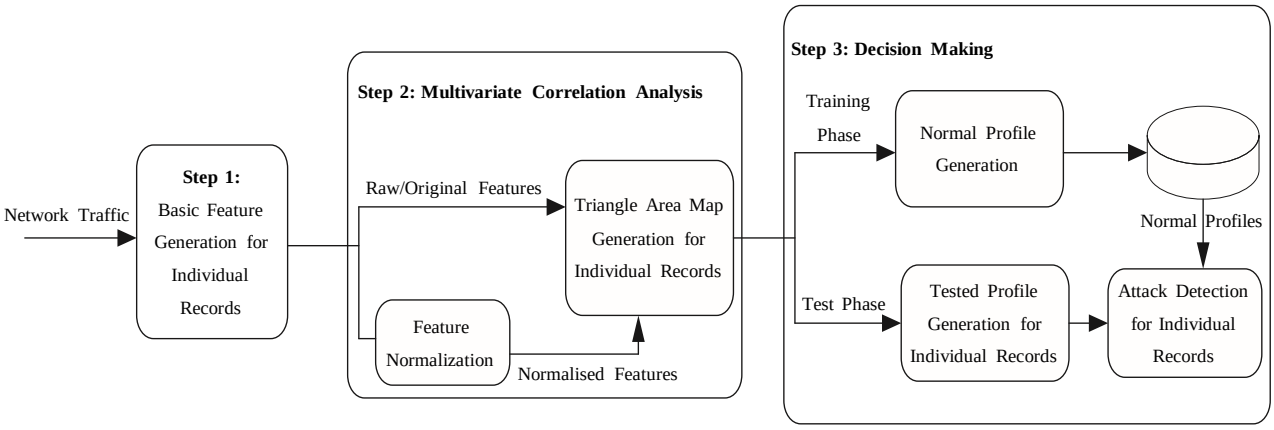
The large-scale deployment of wireless sensor networks (WSNs) and the need for data aggregation necessitate efficient organization of the network topology for the purpose of balancing the load and prolonging the network lifetime. Clustering has proven to be an effective approach for organizing the network into a connected hierarchy. In this article, we highlight the challenges in clustering a WSN, discuss the design rationale of the different clustering approaches, and classify the proposed approaches based on their objectives and design principles. We further discuss several key issues that affect the practical deployment of clustering techniques in sensor network applications.

## II. ORGANIZATION OF PAPER

Intrusion detection in such systems has been an active area of research, while the problem of automated response has received relatively less attention. The thought often is that a system administrator will be included in the loop for troubleshooting once the alert about a possible intrusion has been raised. In this paper propose two algorithms are Signature based instruction, IDPS (Intrusion detection and prevention system). Implementing a Signature based rule, this allows us to construct if-then rules that reflect common ways of describing security attacks.

IDP system is automatically to eliminate the harm of attacks and adopts the distributed architecture to monitor intrusion activities and realize abnormal events processing in local nodes

Framework of the proposed distributed denial-of-service attack detection and prevention system




Finally, the system is analysed and verified. The simulation results indicate that the compromised nodes can self-recover effectively and network total energy consumption also is reduced effectively.

In IDPS (Intrusion detection system) watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDPS block the attacker node and remove from the DDOS attack.

## III. DETECTION MECHANISM

### 3.1 MCA (Multivariate Correlation Analysis)

The coefficient of multiple correlation is a measure of how well a given variable can be predicted using a linear function of a set of other variables. It is measured by the square root of the coefficient of determination, but under the particular assumptions that an intercept is included and that the best possible linear predictors are used, whereas the coefficient of determination is defined for more general cases, including those of nonlinear prediction and those in which the predicted values have not been derived from a model-fitting procedure. The coefficient of multiple correlation takes values between zero and one a higher value indicates a better predictability of the dependent variable from the independent variables, with a value of one indicating that the predictions are exactly correct and a value of zero indicating that no linear combination of the independent variables is a better predictor than is the fixed mean of the dependent variable. The present a threshold-based detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records.

#### *3.1.1 Normal Profile Generation*

Mahalanobis Distance (MD) is adopted to measure the dissimilarity between traffic records.

Assume there is a set of *g* legitimate training traffic records

$Xnormal = \{xnormal_1, xnormal_2, \cdots, xnormal_g\}$.

#### *3.1.2 Sample-By-Sample Detection*

Systematically proved that the group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism. To better understand the merits, we illustrate them through a mathematical example given in which assumes traffic samples are independent and identically distributed and legitimate traffic and illegitimate traffic follow normal distributions.

**Normal Distributions**

$$X_1 \sim N(\mu^1, \sigma^1 2) \quad \text{and}$$

$$X_2 \sim N(\mu_2, \sigma^2 2)$$

the two distributions are described statistically using the probability density functions and

$$f\left(x; \mu_{1,\sigma_1^2}\right) = \left(\frac{1}{\sigma_1 \sqrt{2\pi}}\right) e^{-(x-\mu 1)^2} \quad / 2\sigma_1^2$$

$$f\left(x;\mu_{2,\sigma_2^2}\right)=\left(\frac{1}{\sigma_2\sqrt{2\pi}}\right)e^{-(x-\mu 2)^2}\ /2\sigma_2^2$$

Respectively, where

$x \in (-\infty,+\infty)$.

In this task, the sample-by sample labelling and the group-based labelling are used to identify the correct distribution for the individuals from a group of $k$ independent samples

$\{x_1, x_2, \cdots, x_k\}$.

probabilities of correctly classifying a sample into its distribution using the sample-by-sample labelling as the cumulative distribution functions

**Cumulative Distribution**

$$P_1=\int_{-\infty}^{\bar{\mu}} 1/\sigma_{1\sqrt{2\pi}}\, e^{-(x-\mu 1)^2\ /2e_1^2}dx,$$

$$P_2=\int_{\bar{\mu}}^{+\infty} 1/\sigma_{2\sqrt{2\pi}}\, e^{-(x-\mu 2)^2\ /2e_2^2}dx,$$

Where

$$\bar{\mu}=\mu_1\ \times\frac{\sigma_2}{\sigma_1+\sigma_2}+\mu_2\ \times\frac{\sigma_1}{\sigma_1+\sigma_2}$$

is the threshold value for classifying a sample into one of the two distributions ($\mu_1,\sigma_1{}^1$) and $N(2_1,\sigma_2{}^2)$.

$$P_1{}^1 = 1- P_1$$

It represents the probability that a sample coming from the distribution $N(\mu_1,\sigma_1{}^2)$ is not correctly classified into $X_1$.

$$P_2{}^1 = 1- P_2$$

It represents the probability that a sample coming from the distribution $N(\mu_2,\sigma_2{}^2)$ is not correctly classified into $X_2$.

The results of classification follow the binomial distribution, the probability of correctly labelling $j$ samples is defined as $Pr(j) = C_k^j P^j(1-P)^{k-j}$ where $j = 1,2,\cdots,k$. Thus, the probability of correctly classifying all $k$ samples is

$Pr(k) = P^k$.

Classify The Same Group Of Independent Samples

$\{x_1, x_2, \cdots, x_k\}$

using the groupbased labeling, a new random variable $z$, which is the mean of $k$ random samples from the distribution $N(\mu_l,\sigma_l^2)$, is defined as

$$z=\frac{1}{k}\sum_{t=1}^{k} x_{t,}$$

where

$x_t \in X_l$ and $l = 1,2$.

Clearly, the new random variable $z$ follows the distribution

$Z_l \sim N(\mu_l, {}_k^1\sigma_l^2)$ in which $l = 1,2$.

The threshold value for classification is

$$\bar{\mu}=\mu_1\ \times\frac{\sigma_2}{\sigma_1+\sigma_2}+\mu_2\ \times\frac{\sigma_1}{\sigma_1+\sigma_2}$$

Since the random variable $z$ is generated utilizing $k$ random samples $x_t$ from the distribution $N(\mu_l,\sigma_l^2)$, the detection precision rate of the $z$ correctly classified into the respective distribution $N(\mu_1,\sigma_1{}^2)$ or $N(\mu_2,\sigma_2{}^2)$ .

$$q_1 = q_{2,}q_1' = 1 - q_1\ and\ q_2' = 1 - q_2$$

### 3.2 IDPS

In IDPS (Intrusion detection and prevention system) we set one node as IDPS node, that node watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack.

#### *3.2.1 IDPS Detection Methodology*

##### *3.2.1.1 Signature-Based Detection*

Compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats.

Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

##### *3.2.1.2 Anomaly-Based Detection*

Sample network activity to compare to traffic that is known to be normal. When measured activity is outside baseline parameters or clipping level, IDPS will trigger an alert.

Anomaly-based detection can detect new types of attacks. Requires much more overhead and processing capacity than signature-based .May generate many false positives.

##### *3.2.1.3 Stateful Protocol Analysis*

A key development in IDPS technologies was the use of protocol analyzers. Protocol analyzers can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behavior or exploits against predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state.

IDPS incorrectly identifies benign activity as being malicious, **a false positive** has occurred. When an IDPS fails to identify malicious activity, **a false negative** has occurred. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other.

***3.2.2 Wireless IDPS***

IDPS monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves.

It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring.

It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring.

For most environments, a combination of network-based and host-based IDPSs is needed for an effective IDPS solution.

NBA technologies can also be deployed if organizations desire additional detection capabilities for DoS & DDoS attacks, worms, and other threats that NBAs are particularly good at detecting.

## IV. EXPERIMENTAL EVALUATION

Ad hoc distance vector routing protocols achieve their best performance when sensor nodes are categorized. Node categorization ensures that the clustering process starts simultaneously throughout the network.

### 4.1 Sensor Node Deployment

Large number of sensor nodes are randomly deployed in a two dimensional area. Each sensor node generates sensory data periodically and all these nodes collaborate to forward packets containing the data towards a sink. The sink is located within the network. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes right after deployment.

### 4.2 Neighbour Distance Calculation

In iterative clustering techniques, a node waits for a specific event to occur or certain nodes to decide their role before making a decision. A node waits for all its neighbours with higher weights to decide to be CHs or join existing clusters. Nodes possessing the highest weights in their one-hop neighbourhoods are elected as CHs.

### 4.3 Cluster Node Formation

To support data aggregation through efficient network organization, nodes can be partitioned into a number of small groups called clusters. Each cluster has a coordinator, referred to as a cluster head, and a number of member nodes. Clustering results in a two-tier hierarchy in which cluster heads (CHs) form the higher tier while member nodes form the lower tier. The member nodes report their data to the respective CHs. The CHs aggregate the data and send them to the central base through other CHs. Because CHs often transmit data over longer distances, they lose more energy compared to member nodes. The network may be reclustered periodically in order to select energy-abundant nodes to serve as CHs, thus distributing the load uniformly on all the nodes

### 4.4 Packet Sending and Forwarding

When a node wants to send out a packet, it attaches to the packet with a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to the cluster head. When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet, and then forwards the packet to its parent. After receiving a packet, the sink decrypts it, and thus finds out the original sender and the packet sequence number.

### 4.5 Node Categorization

In this module, to identify nodes those are droppers/modifiers for sure or are suspicious droppers/ modifiers. Behaviors of sensor nodes can be observed in a large variety of scenarios. In every round, for each sensor node, the sink keeps track of the number of packets sent from sensor node, the sequence numbers of these packets, and the number of flips in the sequence numbers of these packets. In the end of each round, the sink calculates the dropping ratio for each sensor node. The dropping ratio in this round is calculated based on the dropping ratio of every sensor node and the cluster based algorithm, the sink identifies the nodes that are droppers for sure and that are possibly droppers.

### 4.6 Hybrid Ranking Algorithm

The bad node modification is done by HR method to reduce packet droppers and modifiers. The suspiciously bad nodes are identified based on the simultaneous selection of nodes for sending packet. For each of these scenarios, node categorization algorithm is applied to identify sensor nodes that are bad for sure or suspiciously bad. After multiple rounds, sink further identifies bad nodes from those that are suspiciously bad by applying several proposed heuristic methods. The tree used for forwarding data from sensor nodes to the sink is dynamically changed from round to round. In other words, each sensor node may have a different parent node from round to round. We rank the suspiciously bad nodes based on their probabilities of being bad, and identify part of them as most likely bad nodes.

## V. CONCLUSION

The problem in our paper however, can be solved by utilizing statistical normalization technique to eliminate the bias from the data. This technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offer extra true characterization for network traffic behaviours. Attacks of internet drain a lot of resources, creation of the victim host cannot accept normal network requests take up a grouping of bandwidth, resulting in substantial losses of economic in network. It is not easy to identify the exact signature of attacking and Intrusion detection systems are a key module in ensuring the safety of networks and systems. Therefore, we propose a signature based Intrusion detection with the interrelation of IP address analysis. This paper focused on distribution of network traffic during the data transmissions using DDOS detection scheme based on the IP address analysis.

The intrusion can be detected using the signature based with analysis of interrelation of IP address. The results have discovered that when working with non-normalized data, our detection system achieves maximum 95.20 percent detection accuracy.

## REFERENCES

[1] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers & Security*, vol. 28, pp. 18-28, 2009.

[2] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[3] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detection using fuzzy association rules," Applied Soft Computing, vol. 9 , no. 2, pp. 462-469, 2009.

[4] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[5] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[6] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.

[7] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[8] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 35 , pp. 302-312, 2005.

[9] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.

[10] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," *Pattern Recognition*, vol. 40, pp. 21852197, 2007.