Detection of denial of service attack using Hamming Distance and cluster Formation

Ankur Sharma[1] Anurag Rana[2] Gourav Tandon[3]
Associate Professor, Assistant Professor , Mtech Scholar
Department of CSE
Arni University

Abstract

Today many applications utilize WSN for real time detection of event. Even from their earliest applications, sensor networks have been targeted for attack by adversaries with interest in intercepting the data being sent, or in reducing the ability of the network to carry out its mission. There are a lot of possible attacks against WSNs, which have different objectives, are performed at different levels, and result in different consequences. Wireless sensors have limited energy and computational capabilities, making many traditional security methodologies difficult or impossible to be utilized. In this work we describe the security goals and DDOS attack in WSN. There are many techniques available that are used to detect DDOS attack in WSN but they all prevent the attack after that has been completely launched. This leads to the loss of data and resources of sensor node consumed more but these resources are limited. So here we introduced a new scheme that early detect DDOS attack using Hamming distance and cluster formation. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Performance of this scheme has been seen on the basis of packet delivery ratio, no. of packets flooded and remaining energy of the network.

Keywords: DDOS, Hamming Distance ,Cluster formation

Introduction

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. The sensor nodes have extreme resource limitations, unreliable communication medium and that too in unattended environments. This makes it very difficult for the implementation of the existing security approaches to WSNs due to the complexity of the existing algorithms.

Algorithms in WSN are categorized on the basis of range based and range free approaches. Range free algorithms are distance independent but ranges based algorithms are dependent upon distance.

1.1 Distances

There are number of distances that impact the performance of the system. The distances can be used to detect the abnormality within the transmitted data. The distances and evaluation equations are discussed in this section.

- Hamming distance

The Hamming distance is one of the commonly used mechanisms to detect the problems within the transmitted data. The Hamming distance depends upon the parity

of data. Parity of data could be even or odd. In case of even parity there are even number of 1s and in case of odd parity there will even number of 1s. The evaluation equation for the hamming distance is given as under

d=min {d(x,y):x,y∈C,x≠y}.

Equation 1: Hamming distance evaluation equations

- Cosine distance

Cosine similarity. **Cosine similarity** is a measure of **similarity** between two non-zero vectors of an inner product space that measures the **cosine** of the angle between them. The **cosine** of 0° is 1, and it is less than 1 for any angle in the interval (0,π] radians. This distance evaluates attacks but with less speed. The evaluation equation for the cosine distance is given as under

$$D_c = 1 - S_c$$

Equation 2: Cosine distance evaluation equation

Where D is the cosine distance and S is the cosine similarity

- Manhatton distance

This distance is simple to evaluate and compares bits of transmitted and received bits. The transmitted bits if different from the received bits then attack is detected. The distance vectors can be denoted with X2 and X1 horizontally and Y1 and Y2 as vertical distance. The evaluation equation for the Manhatton distance is given as under

M=(X2-X1)+(Y2-Y1)

Equation 3: Manhatton distance evaluation equation

Where M is the manhatton distance, X2 , X1 are horizontal vector of transmitted data and Y1, Y2 are vertical vector of transmitted data.

- Minkowsky Distance

The **Minkowski distance** is a metric in a normed vector space which can be considered as a generalization of both the Euclidean **distance** and the Manhattan **distance**. The Minkowsky distance is evaluated through the following equation

$$D(X,Y) = \sum |(x_i - y_i)^p|^{\frac{1}{p}}$$

Equation 4: Minkowsky distance evaluation equation

Where x and y is the distances between the sender and receiver. 'p' is the normal vector.

ATTACKS IN WSN

Due to the unique characteristics of underlying networking protocols, sensor networks are vulnerable to security threats. Attacks can occur at any layer such as physical, link, network, transport, and application etc. Most of these routing protocols are not designed to have security mechanisms and it makes it even easier for an attacker to break the security for example, attacks at the physical layer of the network include jamming of radio signal, tampering with physical devices etc. In the following section we discuss in detail the layer wise attacks in WSNs

A. Physical layer attacks

- Jamming – It is caused due to interference with the radio frequencies of the network's devices which is an attack on the availability of the sensor network. It is different from normal radio propagation in the way that it is unwanted and disruptive, thus resulting in denial-of-service conditions.
- Tampering – It is also called node capturing in which a node is compromised, it is easy to perform and is pretty harmful. Tampering is physically modifying and destroying sensors nodes.

B. Link layer attacks

- Collision – It is caused in link layer that handles neighbor-to-neighbor communication along with channel arbitration. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission, CRC mismatch and

possibly require retransmission can be caused by a single bit error.

- Exhaustion – Exhaustion of a network's battery power can be induced by an interrogation attack. A compromised node could repeatedly send thus consuming the battery power more than required

C. Network layer attacks

- Hello flood attack – It is caused when an attacker with high transmission power can send or replay hello packets which are used for neighbour discovery. In this way, attacker creates an illusion of being a neighbor to other nodes and underlying routing protocol can be disrupted which facilitate further types of attacks.
- Wormhole attack – It is caused due to formation of a low-latency link that is formed so that packets can travel from one to the other end faster than normally via a multi-hop route. The wormhole attack is a threat against the routing protocol and is challenging to detect and prevent. In this type of attack, an adversary can convince the distant nodes that are only one or two hops away through the wormhole causing confusion in the network routing mechanisms.
- DDOS attack- Distributed denial of service attack is caused due to high congestion and denial of services to the users. The traffic is jammed in this cased and hence users may not get the resources they require. The performance degrades in terms of cost and energy consumption.
- Sybil attack – It is caused when an attacker uses a malicious device to create a large number of entities in order to gain influence in the network traffic. The ID of these malicious nodes can be the result due to fake network additions or duplication of existing legitimate identities. The sybil attack usually targets fault tolerant schemes including distributed storage, topology maintenance, and multi-hop routing.

Literature Survey

WSN is vastly used area and distinct users interacting with it. In order to resolve the problem associated with attacks in WSN various techniques are proposed. This literature studies the such mechanisms.

[7] Proposed a generalized attack detection model that utilizes the spatial correlation of received signal strength inherited from wireless nodes. The suggested work provide a theoretical analysis of our approach. We then derive the test statistics for detection of identity-based attacks by using the K-means algorithm. The proposed attack detector is robust when handling the situations of attackers that use different transmission power levels to attack the detection scheme. We further describe how we integrated our attack detector into a real-time indoor localization system, which can also localize the positions of the attackers.

Identity based attack detection process uses detection but blocking process is missing. Median error can still be minimized.

[8] In this paper, a distributed method has been presented using mobile agents and local information of each sensor to detect DDOS attack. The method presented in this paper re-moves the adversary nodes from participation in routing while using mobile nodes and increases the security in network.

This work improves packet drop ratio but intrusion detection and blocking of nodes being is missing hence further improvement in terms of blocking by establishing threshold in not done. Hence throughput can further be improved.

[9] Proposed a fully distributed and effective scheme that randomly drops extra PKC request messages beyond its processing capability. This approach is not only resistant to PKC-based DoS attacks, but also energy-efficient.

The residual energy is not considered hence by considering this energy effect further energy consumption can be minimized.

[10] In this paper, we propose a source-authenticated broadcast encryption scheme by fixing the identity-based broad- cast encryption scheme. The security of this scheme is proved in the random oracle model. Analysis of our scheme shows that it is comparatively efficient in terms of computation and communication.

Key based approach is used in which energy consumption art source end is high. Energy consumption in resource constraint environment can further be minimized.

[11] The proposed scheme, does not need issuing a third-party query to certificate authority (CA). Moreover, it eliminates the key escrow problem, an important constraint in Identity-based digital signatures. Also, the sender has the ability to update its keys without changing its identity whenever necessary.

Digital signatures scheme is one of the most secure schemes to ensure attack prevention. This approach is sender based however intermediate attacks can occur and also energy consumption is high.

[12] The so-called indirect DDOS attack is the main focus of this study. A performance analysis is devised, where the expected potential number of indirect DDOS nodes in randomly deployed WSNs is computed. Moreover, the probability of an (indirect) DDOS-free sensor network is calculated subject to the number of sensor nodes and the sensor area intensity. Specific sensor nodes are dealt with in this approach.

Proposed Work

DDOS Algorithm is a range based algorithm. In range based algorithm only use range measurement whereas range free algorithm consider content of the message. DDOS Attack algorithm is created for detecting and removing wormhole attack. In our algorithm we have included NCA also. NCA means node capture attack. In Node capture attack, a node is captured and then falsifying information is given about the node. The node capture attack will make the attacker grab the information about the particular node and replace the existing node with the malicious node. The malicious node then act in place of the other node. The malicious activity performed by the node will make the actual node to be accounted for and punished. In order to resolve the problem random key will be utilized. The KNN with random key hence is proposed.

5.1 Algorithm

The existing algorithm will be as follows

a) Assign the Ids to the nodes.
b) Detect the malicious Entry
c) If Malicious(Node) then
d) Block the node
   Else
e) Move onto next step in sequence
   End of if
f) Calculate localization Error
g) Stop

In the existing system random keys are not considered. in the proposed system random ids for the nodes are considered. In the proposed algorithm we will consider the following steps

h) Generate random Ids for the nodes.
i) Assign the Ids to the nodes.
j) Detect the malicious Entry
k) If Malicious(Node) then
l) Block the node
   Else
m) Move onto next step in sequence
   End of if
n) Calculate localization Error
o) Stop

The above algorithm will be used to determine whether the attack has occurred on the node or node. If attack does occurred on the system than node which is malicious is blocked. Otherwise node is allowed to perform the suggested operation. In the end localization error will be calculated. From the experiment it is proved that localization error in case of proposed system is less as compared to the previous algorithm

More elaborated structure is presented in the following flowchart. The flowchart describes the process of localization and how the problem is going to be resolved. The localization process will help in finding the position of the unknown nodes. The intruder cannot enter into the system by the use of proposed system.

Results

DDOS attack will be the one in which one node takes the identity of other node. The overall performance goes down by the application of DDOS attack. In order to resolve the problem Euclidean distance mechanism is merged along with KNN approach. KNN used to find the neighbors of the node being analyzed. Incase their exist only one neighbor of current node then DDOS attack is detected the Euclidean distance is used to check the location of the DDOS node. The overall time consumption of simulation is achieved to be better as compare to existing approach. This is shown as under

Table 1: Showing time consumption of existing and proposed system

PROPOSED KNN+EUCLIDEAN	EXISTING KNN
12.5357	22.4715
36.6243	44.4277
48.6805	64.4345
46.7414	60.4107
73.0829	98.9666
101.205	113.473

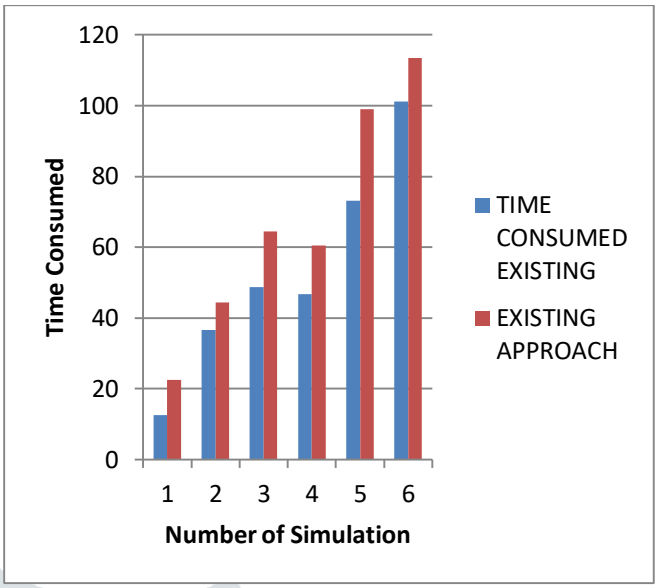

Figure 1: Showing time consumption of existing and proposed system

Conclusion

The proposed work efficiently analyse the DDOS attack. Strategy to tackle DDOS attack is suggested. Using the methodology lifetime of the network can be considerably enhanced. Packet drop ratio which is the problem in existing research is also tackled. Static nodes are considered and handled in existing scheme of thing but this approach analyse various distances and then suggest best possible distance based approach for attack detection.

In future K means clustering technique can be used along with KNN_Euclidean distance approach to further classify and analyse the adverse affects of DDOS attacks.

References

[1] C. Wang, W. S. Kennedy, and C. A. White, "A New Family of Near-metrics for Universal Similarity," *IEEE Access*, vol. 07974, pp. 1–26, 2017.

[2] Z. Zhou, C. Du, L. Shu, G. Hancke, J. Niu, and H. Ning, "An Energy-Balanced Heuristic for Mobile Sink Scheduling in Hybrid WSNs," *IEEE Trans. Ind. Informatics*, vol. 12, no. 1, pp. 28–40, 2016.

[3] W. Wang and Y. Zhang, "On fuzzy cluster validity indices," *Fuzzy Sets Syst.*, vol. 158, no. 19, pp. 2095–2117, 2007.

[4] S. P. Chatzis, "A fuzzy c-means-type algorithm for clustering of data with mixed numeric and categorical attributes employing a probabilistic dissimilarity functional," *Expert Syst. Appl.*, vol. 38, no. 7, pp. 8684–8689, 2011.

[5] A. Fahad, N. Alshatri, Z. Tari, A. Alamri, I. Khalil, A. Zomaya, S. Foufou, and A. Bouras, "A Survey of Clustering Algorithms for Big Data : Taxonomy & Empirical Analysis," *IEEE Access*, 2014.

[6] W. Chen, S. Member, R. Ferreira, E. Deelman, and T. Fahringer, "Dynamic and Fault-Tolerant Clustering for Scientific Workflows," vol. 7161, no. FEBRUARY, pp. 1–14, 2015.

[7] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, 2010.

[8] S. Moradi, "A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks," pp. 276–280, 2016.

[9] D. Kim and S. An, "PKC-based dos attacks-resistant scheme in wireless sensor networks," *IEEE Sens. J.*, vol. 16, no. 8, pp. 2217–2218, 2016.

[10] M. Luo, C. Zou, and J. Xu, "An efficient identity-based broadcast signcryption scheme," *J. Softw.*, vol. 7, no. 2, pp. 366–373, 2012.

[11] S. Sadrhaghighi and I. T. Engineering, "Detect Pollution Attacks in Intra-Session Network Coding," pp. 7–12, 2016.

[12] P. Sarigiannidis, "Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks," pp. 0–5, 2016.

[13] S. Mahajan, "A Mechanism of preventing Sybil Attack in MANET using Bacterial Foraging Optimization," pp. 4–8, 2016.

[14] N. Alsaedi, F. Hashim, and A. Sali, "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks," no. Micc, pp. 91–95, 2015.