A Study of Attack Detection and Localization Scheme Using Enhanced Hash Technique

Prof. Sunny G. Gandhi
Assistant Professor
D.M.I.E.T.R, Sawangi (M), India
Sunnygandhi09@gmail.com

Prof. Anand G. Sharma
Assistant Professor
S.S.G.M.C.E. , Shegaon, India
Sharma.anand2008@gmail.com

Abstract: Security plays an vital role in wireless sensor networks. The nodes are deployed in the physical environment. Hackers may easily access the data. In order to provide security, The Advanced Encryption Standard (AES) algorithm has developed into an option for various security services. Sensor nodes collect the data from the environment and send to sink. But attackers corrupt data while transmitting therefore data security is main concern of wireless sensor network (WSN). Owing to the increasing popularity of wireless sensor networks, they have become attractive targets for malicious attacks. Due to the ad-hoc nature and openness of wireless sensor networks, they are susceptible to the identity based attack. In this paper, we study on a process of named Attack Detection and Localization Scheme to detect and localize the identity based attacks. An improved algorithm for hashing has been proposed. We named it as Effective Hashing Technique (EHT).It generates the Hash keys to differentiate an attacker from a normal node and to reduce the occurrences of any false positives or negatives. Also, our localization algorithm efficiently finds out the position estimates for the nodes.

Keywords: *ADLs, RSSs, EHTs.*

*****

I. INTRODUCTION

A Sensor network is a collection of densely populated small devices, which collect information from an area under observation and send it to destination. Wireless sensor networks make easier monitoring and controlling of physical environments from remote locations with better quality. Security is the major concern of these networks especially in unattended areas. The sensor nodes forward data from the area under observation to the base station so that it can get regular reports of the activities occurring there. This requires a high level of cooperation among all the participating nodes.[2] WSN has sensor nodes that sense the environment parameters like temperature, humidity, pollution etc. and send the collected data to sink. But during transmission of data there is high threat on data as many intruders are waiting for chance to attack the data. Therefore WSN has high network security issue. So, some mechanism is necessary to maintain authenticity, data integrity and confidentiality. [4]. Wireless Sensor Networks are consist of sensors which are distributed in an ad-hoc sequence manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. Wireless sensor networks consist of protocols and algorithms with self-organizing power. A base station is able to handle over the particular region. In order to make a very few messages sent and save energy, sensor readings from different types of nodes in process at the many possible formatting points. An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. The applications of wireless sensor can be divided in three categories. They are: Monitoring of objects, Monitoring of an area, Monitoring of both area and objects. Monitoring objects are Structural Monitoring, Eco-physiology, Condition based Maintenance, Medical Diagnostics, Urban terrain mapping. The user sends the data in a wireless sensor network with secure manner by using non-linear AES Algorithm. [3]. WSNs are vulnerable to security attacks from the adversaries that are posing a threat to the identity of node. If proper security management schemes are not practiced, it can severely degrade the performance of the network. Thus, it is important that a WSN must be able to distinguish the legitimate nodes and the adversaries posing to be legitimate members of the network.

In this paper, we study about an Attack Detection and Localization Scheme (ADLS) that can detect and localize the multiple identity-based attacks like spoofing and prevent any occurrences of false positives or negatives using Hash keys assigned to different nodes and generated by our EHT algorithm.

II. RELATED WORK

[A]. Generalized Attack Detection Methods

Received Signal Strength (RSS):

RSS is the power of the signal at the receiver. During propagation of the signal from the sender to receiver, multiple environmental phenomena modify the transmitted signal strength. For example, in closed room, pass the signal will be reflected on a wall. This reflected signal can then interfere with the original signal constructively or destructively resulting in modified signal intensity. Similarly an prevent in the path may create a dark area of low signal power on the side of the prevent away from the sender. Transmitted signals also suffer from absorption and attenuation which further reduce signal strength. The combined effect of all the RSS values reduced exponentially with distance. In fact, as we changes from the sender, the RSS values drop rapidly initially. However, after some distance, the signal to noisy ratio decreases to the sensitivity of the receiver and, hence, the RSSI values visible fairly constant to the sender. Therefore, the RSS values are highly dependent on environment phenomena. This reliance of RSS values on the environmental phenomena make it too much tough for the introducer to spoof RSS values.

Attack Detection Using Cluster Analysis:

Cluster analysis is required once the signal strength from the nodes is obtained. RSS-based spatial correlation receiver titled from wireless node to performed spoofing attack detection. [6] But the RSS readings from a wireless node may vary and should cluster together. RSS read over a time from the same physical location which will belong to the same cluster points in the n-dimensional signal space, on the other side RSS readings from different locations over time should form different clusters in signal space. In spoofing attack, the same ID to transmit data packets is used by the harmed person and the attacker, and the RSS reading of that ID is the mixture reading measured from each personal node. In a spoofing attack, the RSS readings from the suffering node and the spoofing attackers are mixed together.

[B].Integrated Attack Detection and Localization

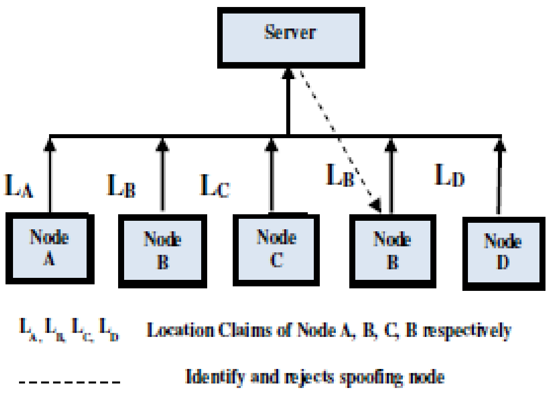
A. *ADLS Architecture*

In a large-scale wireless sensor networks, multiple attackers may impersonate as the same legitimate node in the network and together may launch malicious large scale attacks like Denial of Service. Therefore, it is necessary to detect the presence of such attacks, determine their numbers and to locate their actual positions so that such kind of attacks can be prevented. In order to accomplish this, we have proposed architecture for our scheme.

The main Objectives of our proposed scheme are:-

- It provides an alternative mechanism to detect the presence of spoofing attacks along with determining the number of attackers and giving their position estimates without the use of any complex cryptographic algorithms.
- Minimizes the infrastructural, computational and management overhead.
- Improves the network throughput and lifetime conservation of the power, bandwidth and other resources available for legitimate users.
- Prevention of large scale network malicious attacks such as Denial of Service Attacks & Network resource utilization attacks or Resource Depletion attacks

The diagrammatic representation is given as under:-


Server
LA
LB
LC
LB
LD
Node A
Node B
Node C
Node B
Node D
L_A, L_B, L_C, L_D Location Claims of Node A, B, C, B respectively
--------- Identify and rejects spoofing node

In the above diagram, the attacker spoofs the node B and claims its location **LB.** The server checks for the identity of the node by using the ADLS and rejects the attacker node[1].

B. *Working Mechanism*

This is a different approach to detect as well as localize the identity based attacks like spoofing. This method utilizes the Hash keys generated by our EHT algorithm to distinguish the legitimate node from the attacker in order to detect the attacker. The location of the attacker can then be found out by verifying its (X, Y) coordinates using our localization algorithm. This also reduces the occurrences of any false positives or negatives.

The working mechanism can be explained with the help of the flow diagram given below. The malicious node claims the location of a legitimate node. It then sends the request to the cluster head where the hash key is verified. If the key is found to be replicated, the message is send to the destination (base station), where the attacker may be identified and its position estimates are given.

C. *Design of Attack Detection and Localization Algorithm*

The generalized algorithm for our proposed scheme is given as under. The first step consists of generating a unique ID for all the nodes in the network using our EHT algorithm. Then, we define our cluster and the nodes in the respective
cluster. Determine the number of clusters in the network. Then, we perform the detection by checking the node key value in every cluster. If any key is found replicated, it detects the presence of an attacker in the network.

GENERALIZED ALGORITHM FOR ADLS

Steps:

Step 1: Generate Unique ID for all nodes in the network using MD5 algorithm

Declare Variables number of node, time and round trip .Input message converted to 128 bits

Input message broken to512-bit blocks called chunks. These are 16, 32-bit little endian MD5 operates 128 bit state. i.e. 4, 32 bit words like A, B, C, D, which are all initialized to fixed constants Main algorithm operates on each 512 bit message block consists of 4 rounds.

Step 2: Define the cluster and the nodes in clusters

Step 3: Let Clusters in Network be 'Cn'

Step 4: For (i=0; i<=Cn)

```
{
AttackerNode A=0;
Perform spoofing attack detection by checking the node
key value in every cluster
A=A++;
//Node, which has replicated key value, is identified as
attacker node
}
```

Step 5: Perform the detection in every cluster

Step 6: Identified number of attackers 'A'

Step 7: Localize the Attacker, by identifying their (X, Y)[1] coordinate values of position.

D. ***Attack Detection using EHT Algorithm***

The ADLS uses the combination of MD5 Hash algorithm and HMAC for the detection of attackers. MD5 hash algorithm creates a 128 bit Hash (fingerprint) value, with input as a string of any arbitrary length. The hash represents a kind of signature for the data. It is used because it's a one way function and it is impossible for the attacker to retrieve the original key value. This is not as

complex as the other cryptographic algorithms, helps in minimizing the overhead for routing and is effective in minimizing the false positives and negatives . We call our algorithm as Effective Hashing Technique (**EHT**)[1]. It is a combination of MD5 & HMAC. The two parts of the algorithm are illustrated individually as below.

HASH ALGORITHM FOR KEY GENERATION

MD5 Hash Algorithm (a)

Input: String of any arbitrary length

Output: 128 bit Hash value

STEPS:

Step1: Set the values for variables i, t, T. Set i=0 & for each t, give the values for all the 64 bits Return T

Step2: For each length, set the time in milliseconds per iteration

Step3: Set the message length and pad length.

Step4: Initialize the 4 state variables, each of which is a 32-bit integer.

P=0x67452301
Q=0xefcdab89
R=0x98badcfe
S=0x10325476

Step5: Group the 512 bit message into 16 different 32 bit slices of data

Step6: Store the "message digest" variables.

PP=P
QQ=Q
RR=R
SS=S

Step7: Let [p, q, r, s, k, j, i] denote the operation:

//Round 1

$\boldsymbol{p = q + ((p + F(q, r, s) + X[k] + T[i]) <<< j).}$

// Use this for 16 operationsset P [expr {$Q + [<<< [expr {$P + [F $Q $R $S] + $X(0)+ $T(1) }] 7]}]

//Round 2

$\boldsymbol{p = q + ((p + G(q, r, s) + X[k] + T[i]) <<< j)}$

// Use this for 16 operations

//Round 3

$\boldsymbol{p = q + ((p + H(q, r, s) + X[k] + T[i]) <<< j)}$

// Use this for 16 operations

//Round 4

$\boldsymbol{p = q + ((p + I(q, r, s) + X[k] + T[i]) <<< j)}$

// Use this for 16 operations

Step8: Update the state variables

P+=PP
Q+=QQ
R+=RR [1]
S+=SS

Step9: Define the functions for the state variables.

$F(x, y, z) = (x \& y) \mid (\sim(x) \& z)$

$G(x, y, z) = (x \& z) \mid (y \& \sim(z))$

$H(x, y, z) = x \wedge y \wedge z$

$I(x, y, z) = y \wedge (x \mid \sim(z))$

E. Localization of Sensor nodes (Attackers)

Localization is the process of finding the location of the sensor nodes. We use multilateration for localization of sensor nodes. Multilateration can be defined as the process of localization that uses the Time Difference of Arrival, for solving the mathematical intersection of multiple hyperbolas Here we use a combination of both mean based and median based localization algorithm to find the position estimates of the nodes. In the mean based technique, the coordinates (X, Y) are based upon the positions of beacon nodes (Boi).Let the distance be Doi and the known position is (Xi, Yi).The position (Xo, Yo) of the node can be found out by finding ( ).This may be calculated using the Least Squares Method. The equation is given as:-

$$Doi = \sqrt{(Xo - Xi)^2 + (Yo - Yi)^2} \quad (2)$$

$$(X^{*} Y^{*}) = \arg.\min(Xo, Yo) \sum_{i=1}^{n} \left[\sqrt{(Xi - Xo)^2 + (Yi - Yo)^2} - Doi\right]^2 \quad (3)$$

Where, i=1, 2 …n

In a situation of no attacks, measurement error may be given by :

$$ei = \sqrt{(Xo - Xi)^2 + (Yo - Yi)^2} - Doi \quad (4)$$

The median value point is a point that is used for the estimation of centre. For the median based localization method, the equation may be given as:-

$$Dom = \sqrt{(X^{m})^2 + (Y^{m})^2} \quad (5)$$

Where, ‘Dom’ is the Euclidean distance [1]

ALGORITHM FOR LOCALIZATION

Input: Nodes that need to be localized
Output: Position estimates (Xo, Yo) for nodes
STEPS:
Step1: Find out the coordinates (Xo, Yo) by selecting every three values from {(Xi, Yi, Doi)}/ i=1, 2...n
Step 2: Then, find the median coordinates ( )
Step 3: For each (Xi, Yi)/ i=1, 2…n, compute the error value

$$ei = \sqrt{(Xo - Xi)^2 + (Yo - Yi)^2} - Doi$$

Where, |*ei*| _ _
Step4: Apply Least mean square error method to find value of (Xo, Yo) as given in the above equation (2)[1]

III. CONCLUSION

We studied the localization attack detection using receiver signal strength (RSS) where the Advanced Encryption Standard (AES) helps to localize the multiple spoofing attacks. Again the ADLS provides an alternative mechanism to detect the presence of spoofing attacks along with determining the number of attackers and giving their position estimates without the use of any complex cryptographic algorithms. Also The ADLS uses the combination of MD5 Hash algorithm and HMAC for the detection of attackers.

REFERENCE

[1]. Ulya Sabeel, Nidhi Chandra, Shivraj Dagadi,” A novel scheme for Multiple Spoof Attack Detection and Localization on WSN-based Home Security System” 5th International Conference on Computational Intelligence and Communication Networks in *Noida, India in* 2013.

[2]. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, and Jerry Cheng,”Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE transactions on parallel and distributed systems, vol. 24, no. 1, January 2013.

[3]. Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[4]. Daniel B. Faria, David R. Cheriton,” Detecting Identity-Based Attacks in Wireless Networks Using Signalprints”, *WiSe'06*, September 29, 2006, Los Angeles, California, USA, Copyright 2006 ACM.

[5]. Sudip Misra, P. Venkata Krishna and Kiran Isaac Abraham, “A simple learning automata based solution for intrusion detection in wireless sensor networks” Wireless Communications and Mobile Computing ,Volume 11, Issue 3, March 2011, Pages: 426–441,

[6]. N Wong, P Ray, G Stephens**,** “Artificial immune systems for the detection of credit card fraud: architecture, prototype and preliminary results”. Information Systems Journal, Vol22, Issue 1, pages 53–76, January 2012.

[7]. Wen Tao Zhu, Yang Xiang, Jianying Zhou, Robert H. Deng, Feng Bao, “Secure localization with attack detection in wireless sensor Networks”, Int. J. Inf. Secur. (2011) 10:155–171, Springer-Verlag 2011.

[8]. Sudip Misra, Ashim Ghosh, A.P. Sagar P., Mohammad S. Obaidat,” Detection of Identity-Based Attacks in Wireless Sensor Networks Using Signalprints”, 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM InternationalConference on Cyber, Physical and Social Computing.

[9]. Yingpei Zeng, Jiannong Cao, Jue Hong, Li Xie, “Secure Localization and Location Verification in Wireless Sensor Networks”,2009 IEEE.