World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:6, No:2, 2012

A Novel Framework for Abnormal Behaviour Identification and Detection for Wireless Sensor Networks

Muhammad R. Ahmed, Xu Huang, Dharmendra Sharma

***Abstract*—**Despite extensive study on wireless sensor network security, defending internal attacks and finding abnormal behaviour of the sensor are still difficult and unsolved task. The conventional cryptographic technique does not give the robust security or detection process to save the network from internal attacker that cause by abnormal behavior. The insider attacker or abnormally behaved sensor identificationand location detection framework using false massage detection and Time difference of Arrival (TDoA) is presented in this paper. It has been shown that the new framework can efficiently identify and detect the insider attacker location so that the attacker can be reprogrammed or subside from the network to save from internal attack**.**

***Keywords*—**Insider Attaker identification, Abnormal Behaviour, Location detection, Time difference of Arrival (TDoA), Wireless sensor network

I. Introduction

WIRELESS sensor network (WSN) consists of spatially distributed autonomous sensors and provide a theoretical basis for many different applications range military implementation in the battlefield, environmental monitoring, health sector as well as emergency response of surveillance. It is an application dependant technology which can be changed and additional sensor nodes can be deployed based on the necessity. The sensor nodes consists a transceiver unit (combination of transmitter and receiver), a restricted memory processing unit, a sensing unit as well as a battery with limited power. Thus, for any application overhead of computation and communication is low. In order to ensure the efficient functionality of WSN, security mechanism is essential, especially in the field of emergency response or battlefield implementations. But security in the wireless sensor network is challenging and important task because of the construction of the node. Many algorithms have developed in order to secure WSN. Most of the work has focused on the pair wise key establishment, authentication access control and defense against attack.

Muhammad R Ahmed is with the Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: muhammad.ahmed@canberra.edu.au)

Xu Huang is with Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: xu.huang@canberra.edu.au)

Dharmendra Sharma is with Faculty of Information Science and Engineering, University of Canberra, Australia, (e-mail: dharmendra.sharma@canberra.edu.au)

Most importantly these works mainly focused on the traditional cryptographic information, data authentication in order to build the relationship between the sensors but the unreliable communication through wireless channel made the techniques vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary [1]. Through this access, the adversaries can easily attack the network internally with data alteration, message negligence, selective forwarding as well as by jamming the network. Adversaries can be determined through the abnormal behaviour of the sensor.

Unfortunately, the internal attack (the sensor behavesabnormally) remains unsolved through the conventional way of WSN security which implements the encrypting method or authentication. Thus, it is important to detect and its location information to provide the complete security to the WSN. [2] In this research work we proposed a twostep method to overcome the security issue. In the first step, the insider attacker or abnormal behavior of the senor will be detected by using the false massage detection process while in the second step the attacker will be located using Time Difference of Arrival (TDoA) triangulation through three beacon nodes location information. With the detection of the abnormal behavior of the sensor (insider attack) and location information a further approach is taken to make the network secure by reprogramming the node or obsolete the node form the network.

The paper is organised as follows: section 2 is comprised of the overview of the related work followed by a description of the proposed framework in section 3. This section covers the details of insider attacker identification process and location detection. The efficiency of the framework is presented in Result section followed by conclusion section 5.

II. Related Works

Numerous ways and solution have been proposed to secure the WSN. So far, security using attacker (abnormal behaviour of the sensor) identification and location discovery has not given significant attention. Even though number of localization process has been proposed in different research but main focus was given on preventing and securing routing from attacks. As the study was done by [3], however, most of the scheme proposed are needed to have special device, such as SeRLoc [4] the improved version of SeRLoc is HiRLoc [5] requires directional antenna, SPINE requires nano second timing scale. Attack resilient location estimation method [6] proposed by Lui fails if the attacker is compromised. ROPE is

combination of SeRLoc and SPINE [7], it require extra hardware and pair wise key with every locator

These developments somehow solve the mathematical problems with certain constrain but does not take the insider attacker identification and location detection in consideration. In our paper we have come up with the approach to identify and detect the internal attacker.

III. Network Model Or Framework Description

A. Assumptions

In our experimental works we use the following parameters: a network with N uniformly distributed sensor node over the area of 500m *500m squared field in a 2D scenario. Sensors and channels are stationary after deployment of the network with transmission radius of 200m. Sensing nodes are responsible to collect and forward the monitored data around them. The collected data is then sent to the sinker through channel. In order to detect the abnormal behavior of the sensor node we use the false massage detection. We will consider the system is synchronized.

B. Abnormal Behaviour/Attacker Identification

The false message or exponential message detection process in a channel is detected with one stationary sinker, in this paper in order to detect the attacker. Insider attacker or abnormal behavior is not possible to detect only based on the cryptographic based technique, as the unreliable wireless channel makes it very easy to compromise the sensors and break the trust relationship established, so the security foundation become insufficient[2]. The false message detection mechanism focuses on the contingency of the message which defines as the exponential message attack. WSN is densely deployed and continuously observe the phenomenon, this characteristics drive the senor nodes network normally encounter the spatio-temporal correlation. In our research we considered the message generated from the nodes is similar for a defined period. In normal massage delivery of the nodes the probability of different message are negligible or rare. If $D$is the length of the message with restricted memory, M_i is the message and F_i is considered as the frequency of the message we can write the Equation below

$$D = \{(M_i, F_i)|(M_1, F_1); (M_2, F_2), \dots\dots, (M_n, F_n)\} \quad (1)$$

It is a set that will store the latest massage that is sent to the network recently. If a new message sent to the network than that is M_{new} arrives at the channel than that is authenticated using the false message detection process [8].

$$match(M_{new}, M_i) = \frac{(V(M_{new}) \times V(M_i))}{(|V(M_{new})| \times |V(M_i)|)} \quad (2)$$

Based on the *k*-nearest neighbour algorithm we can find the normal message from the equation (2), this is the simple algorithm that classifies the data based on neighbour training example [9].

In which $M_i$will be equivalent to$D$, and if the result of the equation (2) match with the threshold than it will be considered as normal massage.The M_{new} will be compared with the whole set of D to determine whether does it match with M_i or not. If it matches it will increase the frequency F_i, or else it will be considered as false message and will be hold in to the buffer until it is authenticated. If it does not match than it will be considered as fake massage and it is the attacker. If the authentication process is not passed it will be considered as a fake message and will be identified as the attacked or abnormal sensor.

In this method the calculation is simpler, the latency is smaller as well as less parameter is considered which is supported by the limited memory sensor nodes [8].

C. Attacker/Abnormal Sensor Location

Location estimation is a complex process that involves multifaceted numerical operations. Unfortunately there is no simple process exists for the efficient computation of a location estimation of wireless sensor nodes. It is uncertain that a more complex mathematical computation will increase the accuracy of the estimation, conversely if a reduction of the complexity that would compromise with the efficiency of location estimation.

In this paper we used the Time Difference of Arrival (TDoA) signal rather than absolute time of Time of Arrival (ToA). A signal is sent to the node by at least three antennas at an unknown and different time. The most common trilateration method is used in order to get the sensor node location [11]. For each TDoA measurement, the transmitter must lie on a hyperboloid with a constant range difference between the two measuring units. If we consider$B_1$is the Master Beacon node. The distance between the source and i^{th}Beacon node is

$$R_i = \sqrt{(X_i - x)^2 - (Y_i - y)^2} \quad (3)$$

In the 2-D scenario the target location can be estimated from the intersection of two TDoA measurements. Beacon nodes (B_1, B_2andB_3) are considered as a measuring unit from which intersection point is determined and that locates the target point A, as shown in figure (1) below:

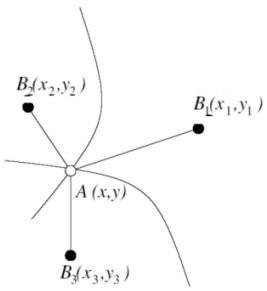

Fig. 1 Attacker Location Detection by beacon nodes

In Figure 1, Three sensors are defined as $B_i$with the location as(x_i, y_i), where i= 1, 2 or 3. For any point $A = (x; y)$in the plane.[11]

The range difference between beacons with respect to the beaconB_i where the signal arrives first, is

$$R_{i,1} = cd_{i,1} = R_i - R_1 \quad (4)$$

where c is the signal propagation speed, $R_{i;1}$is the range difference distance between the first beaconB_1 and the i^{th} beacon$(B_{1(i>1)})$, R_1 is the distance between the first beacon and the source, and $d_{i;1}$is the estimated TDOA between the first beacon$B_1$and the i^{th}beacon$(B_{1(i>1)})$,. This defines the set of nonlinear hyperbolic equations whose solution gives the 2-D coordinates of the source

Solving the nonlinear equations of (4) is dificult. Consequently, linearizing this set of equations is commonly performed. One way of linearizing these equations is through the use of Taylor-series expansion and retaining the first two terms [12,13]. A commonly used alternative method to the Taylor-series expansion method, presented in [14, 15, 16, 17], is to first transform the set of nonlinear equations in (4) into another set of equations. Rearranging the form of (4) into

$$R_{i,1}^2 = (R_{i,1} + R_1)^2 \quad (5)$$

Subtracting (3) at $i = 1$ from (5) results in

$$R_{i,1}^2 + 2R_{i,1}R_1 = X_i^2 + Y_i^2 - 2X_{i,1}x - 2Y_{i,1}y + x^2 + y^2 \quad (6)$$

where $X_{i;1}$and $Y_{i;1}$are equal to X_i- $X_1$and $Y_i$and Y_1respectively. The set of equations in (6) are now linear with the source location $A = (x; y)$and the range of the first receiver to the source R_1as the unknowns, and are more easily handled.

Inorder to solve the R_1we use Chan's method, in this method a non-iterative solution to the hyperbolic position estimation problem which is capable of achieving optimum performance for arbitrarily placed sensors was proposed by Chan [18]. The solution is in closed-form and valid for both distant and close sources. When TDOA estimation errors are small, this method is an approximation to the maximum likelihood (ML) estimator.

Following Chan's method [18], for a three beacon node system ($B = 3$), producing two TDOA's, x and y can be solved in terms of $R_1$from (6). The solution is in the form of

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} X_{2,1} & Y_{2,1} \\ X_{3,1} & Y_{3,1} \end{bmatrix}^2 \times \left\{ \begin{bmatrix} R_{2,1} \\ R_{3,1} \end{bmatrix} R_1 + \frac{1}{2} \begin{bmatrix} R_{2,1}^2 - K_2 + K_1 \\ R_{3,1}^2 - K_3 + K_1 \end{bmatrix} \right\} \quad (7)$$

Where,

$$K_1 = X_1^2 + Y_1^2$$
$$K_2 = X_2^2 + Y_2^2$$
$$K_3 = X_3^2 + Y_3^2$$

When (7) is substituted into (3), with $i = 1$, a quadratic equation in terms of R_1 is produced. Substituting the positive root back into (7) results in the final solution. Therefore, we can find the location of the abnormal node which is $A(x; y)$

IV. Result

In the experiment we have considered the temperature measurement field; the sensors are randomly deployed in the field and assumed that in the field the temperature would be 8 to 14. At the beginning the test was done with 10 sensors where node 4 has different data and secondly with 20 sensors in which node 13 has different data to detect the false message in the Matlab environment. The result shows that it can detect the false massage is detected efficiently with the output massage neighbor node number to determine the neighbor euclidian distance used.

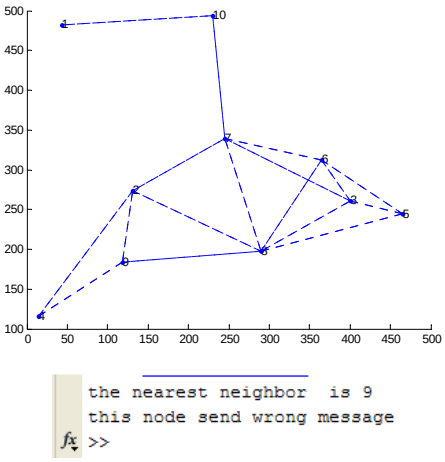

Fig. 2 10 nodes deployed in the sensor field

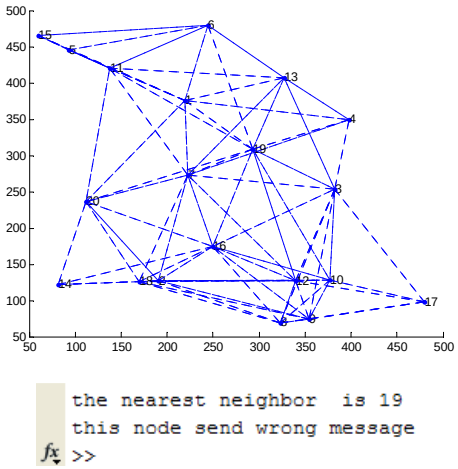

Fig. 3 20 node deployed in the sensor field

When we determined with the false massage we can use the TDOA process to get the location by using equation (7), which is discussed in section 3.

V. Conclusion

In this paper we have presented a novel framework to identify and locate the insider attacker that behave abnormally in the network in the wireless sensor network by using false massage detection and Time Difference of Arrival (TDoA) method, the most common practice in wireless communication to detect the location. Due to the simplicity of the process this method may be useful for the small scale deployment. This

process in for the stationary sensors in future we will implement the process for mobile scenario.

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, 3rd Quarter 2008.

[2] W. T. Zhu, Y. Xiang, J. Zhou, R. H. Deng, and F.Bao, "Secure localization with attack detection in wireless sensor networks," *International Journal of Information Security*, vol. 10, no. 3, pp. 155-171, 2011.

[3] A. Srinivasan, and J. Wu, "A Survey on Secure Localization in Wireless Sensor Networks," *Encyclopedia of wireless and mobile communications*, 2008.

[4] L. Lazos, and R. Poovendran, "SeRLoc: Secure range independent localization for wireless sensor networks," in *ACM workshop on Wireless security (ACMWiSe '04)*, Philadelphia, 2004.

[5] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, February 2006.

[6] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," in *Proc. of The Fourth International Conference on InformationProcessing in Sensor Networks (IPSN '05*), 2005, pp. 99-106.

[7] S. Capkun and J.-P.Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proc. of IEEE INFOCOM '05*, 2005.

[8] Y. Zhang, W. Yang, K. Kim, and M. Park, "Inside attacker detection in Hierarchical Wireless Sensor Networks," in *Proc. of the 3rd International conference on innovative computing information and control (ICICIC)*, 2008.

[9] C. Haiguang, C, XinHua, and N. Junyu, "Implicit Security Authentication Scheme in Wireless Sensor Networks," in *Proc. of 2010 International Conference on Multimedia Information Networking and Security*, 2010.

[10] Y. Chraibi, "Localization in wireless sensor networks," Masters' degree project submitted to KTH signal and sensor systems, Stockholm, Sweden, 2005.

[11] X. Xiaochun, R. Nageswara, and S. Sartaj, "A computational geometry method for DTOA triangulation," in *Proc, of 10th International Conference on Information Fusion*, 2007, pp. 1–7.

[12] W. H. Foy, "Position-Location Solutions by Taylor-Series Estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-12, pp. 187-194, March 1976.

[13] D. J. Torrieri, "Statistical Theory of Passive Location Systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-20, no. 2, pp. 183-198, March 1984.

[14] B. Friedlander, "A Passive Localization Algorithm and Its Accuracy Analysis," *IEEE Journal of Oceanic Engineering*, vol. OE-12, no. 1, pp. 234-244, January 1987.

[15] H. C. Schau, and A. Z. Robinson, "Passive Source Localization Employing Intersecting Spherical Surfaces from Time-of-Arrival Differences," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. ASSP-35, no. 8, pp. 1223-1225, August 1987.

[16] J. O. Smith, and J. S. Abel, "The Spherical Interpolation Method for Source Localization," *IEEE Journal of Oceanic Engineering*, vol. OE-12, no. 1, pp. 246-252, January 1987.

[17] J. S. Abel and J. O. Smith, "The Spherical Interpolation Method for Closed-Form Passive Localization Using Range Difference Measurements," in *Proc. ICASSP-87*, Dallas, TX, 1987, pp. 471-474.

[18] Y. T. Chan and K. C. Ho, "A Simple and Efficient Estimator for Hyperbolic Location," *IEEE Transactions on Signal Processing*, vol. 42, no. 8, pp. 1905-1915, August 1994.