Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2017, Vol. 13(11)

DOI: 10.1177/1550147717740072
journals.sagepub.com/home/ijdsn
SAGE

Detection of attacker and location in wireless sensor network as an application for border surveillance

Mohammed Aseeri[1], Muhammad Ahmed[2], Mohammed Shakib[3], Oussama Ghorbel[4] and Hussian Shaman[1]

Abstract

Border surveillance is one of the high priority in the security of countries around the world. Typical and traditional border observations involve troops and checkpoints at borders, but these do not provide complete security. One effective solution is the addition of smart fencing to enhance surveillance in a Border Patrol system. More specifically, effective border security can be achieved through the introduction of autonomous surveillance and the utilization of wireless sensor networks. Collectively, these wireless sensor networks will create a virtual fencing system comprising a large number of heterogeneous sensor devices. These devices are embedded with cameras and other sensors that provide a continuous monitor. However, to achieve an efficient wireless sensor network, its own security must be assured. This article focuses on the detection of attacks by unknown trespassers (perpetrators) on border surveillance sensor networks. We use both the Dempster–Shafer theory and the time difference of arrival method to identify and locate an attacked node. Simulation results show that the proposed scheme is both plausible and effective.

Keywords

Wireless sensor networks, border surveillance, Time difference of arrival, Dempster–Shafer theory

Date received: 28 February 2017; accepted: 5 October 2017

Handling Editor: Miguel Torres-Ruiz

Introduction

Wireless Sensor Networks (WSNs) applications have attracted researchers worldwide greatly because of their application in numerous scenarios.[1] Area monitoring is regard as one of their new and interesting application domains. WSNs have the capability to monitor and send information autonomously, even in critical and hostile environments. One such application of WSNs is border surveillance. Here, the goal is to detect and signal the presence of trespassers (perpetrators) within a specific area that has been predefined to the WSNs. However, the open nature of WSNs allows the possibility of malicious interference or compromise. This necessitates implementation of high-level security and robustness, especially in malicious environments. That is, for WSNs to function effectively in such malicious environments, security mechanisms are essential.[2] There are several characteristics of WSNs are required, namely, low-cost, energy-efficient, computational power efficiency, communication capabilities in short range, security and privacy mechanism, distributed sensing and processing capabilities, dynamic network topology, self-organization, multi-hop communication,

[1]King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia
[2]University of Portsmouth, Portsmouth, UK
[3]University of Malaya, Kuala Lumpur, Malaysia
[4]University of Sfax, Sfax, Tunisia

Corresponding author:
Mohammed Aseeri, King Abdulaziz City for Science and Technology, P.O. Box 6086, Riyadh 11442, Saudi Arabia.
Email: masseri@kacst.edu.sa

application oriented, robust operations, and small physical size.

Typically, the sensor nodes communicate with each other via multiple hops over an open wireless channel. This presents a security challenge as, on borders, WSNs are normally deployed in an unattended area that is also hostile. Moreover, the sensor nodes do not usually have any physical protection. Consequently therefore, WSN nodes can be easily captured by trespassers, thereby providing trespassers with full access to nodes and the ability to cause a failure of the entire network.

Designing and testing a new WSN algorithm is extremely challenging and maintenance of security integrity ranks as a major concern. Common security threats include selective forwarding, sinkhole attacks, Sybil attacks, wormholes, and a HELLO flood attack.[3] The time difference of arrival (TDoA) triangulation through three beacon nodes location information, is used to detect the attacker location. TDoA technology has been widely used in positioning and navigation system recently. The position estimation of a source through determining TDoA of its signal among distributed sensors has many applications in civil as well as in the military with the detection of the abnormal behavior of the sensor (in-sider attack) and location information. The system that uses TDoA to find a source location it requires at least three sensors one of them is a master (reference) and the other two are slave (auxiliary) sensors. When the location is detected, a further approach is taken to make the network secure by reprogramming the node or obsolete the node from the network. In this article, we have focused on border protection using secure WSNs. To provide that protection, we need the ability to continuously determine whether any node has been attacked. To this end, we have employed the Dempster–Shafer theory (DST) to combine evidence from multiple neighbor nodes to determine whether a given node has been attacked. DST has the capability of modeling the uncertainty in the situation where the independent evidences are limited. WSNs are the most uncertain application scenario. Subsequently, the TDoA method is utilized to find the location of the given node as it has the simplicity. Overall, the implemented method has low latency and computation.

Related work

The researchers have recently investigated WSN-based border protection. In 2004,[4] researchers at Ohio State University deployed sensors with the ability to detect metallic objects, the major goal was to detect the tanks and the vehicles. In 2011, researchers at the University of Virginia, in collaboration with Carnegie-Mellon University, utilized energy-efficient WSNs to detect objects moving through a passage line.[5] Their sensor nodes had embedded sound, photographic, and magnetic sensors. In 2012, German researchers investigated irregularly shaped areas and deployed WSNs[6] to detect trespassers. They utilized multiple sensors to work in a distributed manner.

Unfortunately, there was not much attention has been given in the literature for protecting a network from enemy manipulation, technically termed an attack. Although some work has been performed on protecting WSNs from attacks, it has not specifically focused on border surveillance scenarios.

Staddon et al.[7] outlined a method to track unsuccessful sensor nodes in a network at a sinkhole. Detection of abnormal behavior relied on the assumption that all sensor node data will be relayed toward the sinkhole via a predefined routing tree. Moreover, the sinkhole must have an overall view of the network topology. With this overall knowledge, the method is capable of identifying failed nodes using a routing update message.

Marti et al.[8] presented a watchdog-like method. The method has a node which listens to the next-hop neighbor nodes' broadcasting transmission behavior. It is capable of identifying a packet-dropping attack. Numerous watchdogs must work together with cooperative behavior in this method. Hence, a collaborative and reputable system is necessary to determine an attacker. Quality ratings of the collaborator nodes are therefore requisite.

Zhang and Lee[9] proposed a technique that is considered pioneer work on intrusion detection in the area of wireless ad hoc networks. The author has investigated a different architecture for cooperative discovery of statistical abnormalities, a defense against attacks on ad hoc routing.

Znaidi et al.[10] first introduced a hierarchical distributed algorithm for detecting node replication attacks using a Bloom filter mechanism and a cluster head selection. The proposed method needs to employ additional clustering algorithm and the authors presented only a theoretical discussion on the boundaries.

Garofalo et al.[11] proposed intrusion detection system architecture designed to ensure a trade-off between different requirements. It is high detection rate obtained through decision tree classification. Unfortunately, in this method the power consumption by the sensor is high, it is not resilient to node failures as it uses a tree classification, with a long delay to send the data to the base station, data overhead is high, and it is costly.

Ahmed and Mahmood[12] has proposed a clustering-based anomaly detection technique based on the pattern data and attacks characteristics. Their method works fine with the DoS attacks but it fails for the other attacks.

The most common contemporary techniques exploit cryptographic primitives. Cryptographic methods use additional information to provide security, such as authentication information. A polluted packet can be filtered out based on the validity of the code from the intermediate node. Nevertheless, these schemes carry substantial computational overhead. Furthermore, the schemes need to send verification information such as hashes and signatures separately, prior to the packet, to maintain reliable communications. Thus, considering the characteristics of WSNs, it is not possible to achieve efficient functionality with these methods.

Coverage and deployment strategy of WSN

Border surveillance requires monitoring every point on the border, regardless of the environmental constraints within a large geographical area. Effective border coverage using WSNs depends on both the connectivity and quality of service (QoS) provided by the networks. A node must be able to connect to its one-hop neighbor and, using multi-hop communication, it should be able to transfer data without any alteration. To achieve effective connectivity for data exchange and QoS, one condition is the efficient deployment of the sensor nodes. During border deployments of WSNs, a primary condition is to deploy the minimum number of sensors that will guarantee optimal coverage of every location on the border with efficiency. WSNs are normally deployed based on the application scenarios and number of sensor nodes required to provide the specific applications with effective connectivity. Deployment techniques can be categorized as sparse or dense. Sparse deployment uses fewer sensor nodes.

Conversely, dense deployment uses a relatively high number of sensor nodes in the given field of interest. Dense deployments are normally utilized where it is mandatory for every event to be observed and detected in a large area. Considering the importance and characteristics of border surveillance, the dense deployment strategy is used. Deployment of the sensors normally decided based on the application scenario. Most cases its done by scattering. Despite their quick deployments and significant advantages, WSNs face various security problems due to their nature and the possibility of the presence of one or more faulty or malicious nodes in the existing network.

Model of border attack

The information collected from WSNs is crucial in making border surveillance decisions; thus, the most critical requirement for WSN design is to maintain a high level of network security. The networks can be hacked by the enemies to eavesdrop or to modify fetches data. They may also choose to physically destroy sensor nodes. As a result, protection should be applied both against physical attackers and malicious nodes. The major goal of the network attacker is to discontinue the area monitoring and stop event detection in the border region. To these ends, attackers typically use the following methods. They discontinue or delay the data packet, the attacker tries to modify the node to so as not to forward detected events to the base station. In addition, attackers may attempt to jam the channel to delay the packet, thereby gaining sufficient time to cross the border.

In physical attacks, attackers can physically destroy the sensor node and take it out of the network. With a camera sensor, they can destroy the camera so that analysis of the suspicious area cannot be performed at the data center.

Case study and assumptions

In this research, we used the physical parameter temperature for the purpose of simulation. Our WSN system was built with one sink node and a random spatial distribution of stationary sensor nodes. We assumed that the one-hop neighbor distance was significant and the neighbor acted as an observer and observed the transmissions of the mistrusted node. The second simplifying assumption is the observed physical parameters at the nodes reasonably met the condition of independent events. The independent events observed by neighbor nodes became the individual pieces of evidence. The decision-making process algorithm about an attacker utilized the DST to combine the independent pieces of evidence. This is exemplified by the simplified case as shown in Figure 1. Here, the neighbors of node *A* are

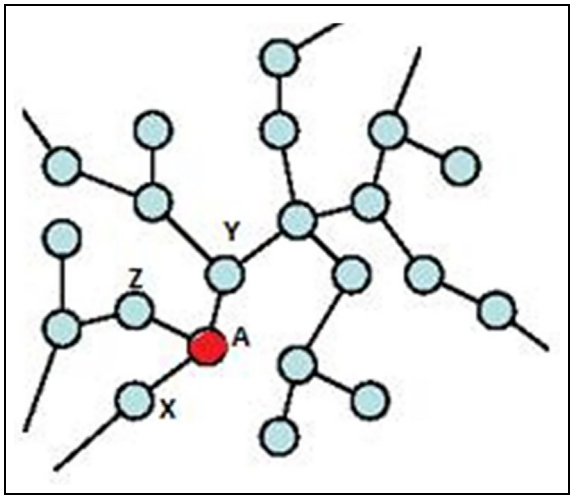

Figure 1. Observation of the attacker with one hop by the neighbor nodes.

X, Y, and Z. They will observe suspected attacked node A for the defined physical parameters of temperature (T) and packet drop rate (PDR).

Methods

The DST was used to detect the attacker. In this theory, the uncertainty interval normally represents probability; probability is replaced by the bounds of belief and plausibility. The lower bound of the interval is known as belief and is characterized by supporting evidence. The interval upper bound is plausibility and is characterized by the un-refuted evidence.[13] The theory is a system of reasoning: the total probabilities of mutually exclusive hypotheses (for independent events) of similar classes are tallied and collected in the frame of discernment, also known as the universal discloser. The basic belief assignment (BBA) or, in other words, function of mass is a function m: $2^{\theta} \rightarrow [0, 1]$, and it satisfies two following conditions

$$m(\phi) = 0 \tag{1}$$

$$\sum_{A \subseteq \theta} m(A_j) = 1 \tag{2}$$

where ϕ is the null set, and a BBA fulfills the condition $m(\phi) = 0$. The basic probability can be rewritten as $m(A)$. This is possible because the share of complete belief allocated to hypothesis A replicates the support as the strength of the evidence. The allocation of belief function maps every hypothesis B to a significant value $bel(B)$ between 0 and 1, defined as

$$bel(B) = \sum_{j:A_j \subseteq A} m(A_j) \tag{3}$$

A plausibility function is considered to be the upper bound of the confidence interval. It accounts for all the observations that do not rule out the given proposal. The plausibility function maps every hypothesis, to a significant value between 0 and 1, and formalized and defined as follows[14]

$$pls(B) = \sum_{j:A_j \cap B \neq \phi} m(A_j) \tag{4}$$

The weight of evidence that is non-contradictory to B is considered the plausibility function. The mathematical relationship concerning the belief and plausibility is given in equation (5)

$$pls(B) = 1 - bel(\sim B) \tag{5}$$

Here, $\sim B$ represents "not B" and represents the hypothesis. Normally, the functions of basic probability number, belief, and plausibility are aligned in element-by-element correspondence. With knowledge of one element or function, the other two functions can be derived.

We assume $m_1(A)$ and $m_2(A)$ are two basic probability numbers, considered to be two independent elements of evidence, meaning that two self-governing neighbor sensor nodes act as observers of the same frame. The conclusions from observations (the pieces of evidence) can be combined in accordance with the evidence theory of Dempster's rule of combination (also known as orthogonal sum), as given by equation (6)

$$(m_1 \oplus m_2)(B) = \frac{\sum_{i,j:A_i \cap A_j = B} m_1(A_i) m_2(A_j)}{1 - \sum_{i,j:A_i \cap A_j = \phi} m_1(A_i) m_2(A_j)} \tag{6}$$

where $\oplus$ denotes Dempster's combination operator that combines two basic probability assignments or BBA into a third.[15] To normalize the equation, a normalization constant L is introduced, as defined by equation (7). More than two belief functions can be combined pairwise

$$L = \frac{1}{K} \tag{7}$$

where

$$K = 1 - \sum_{i,j:A_i \cap A_j = \phi} m_1(A_i) m_2(A_j)$$

The rule of combination assigns belief based on the degree of conflict between pieces of evidence. It also assigns the remaining unused belief to the environment and not to a common hypothesis. This enables the combination with most belief allocated to the disjoint hypothesis and with no reaction of an unreasonable behavioral phenomenon. Belief is similar to confidence levels or evidence.[16] The disagreement between the two belief functions bel_1 and bel_2 is represented by $Con(bel_1, bel_2)$ and is specified by the logarithm of normalization constant,[5] as given in equation (8)

$$Con(bel_1, bel_2) = \log(L) \tag{8}$$

If there is no disagreement between bel_1 and bel_2, then $Con(bel_1, bel_2) = 0$; if there is no commonality between two pieces of evidence, $Con(bel_1, bel_2) = \infty$.[17] Hence, DST integrates ambiguity from contradictory evidence. Following the previous reference, a Dempster–Shafer combination may be formulated as equation (9)

$$m(B) = (m_1 \oplus m_2)(B) = \frac{L \sum_{i,j:A_i \cap A_j = B} m_1(A_i)\, m_2(A_j)}{1 + \log(L)} \tag{9}$$

The DST was applied to the proposed system by treating an independent event as temperature (T) and packet drop rate (PDR). In our application scenario, the set of local elements that are the frame of discernment or the universal discloser can be observed by neighbor nodes within one-hop distance. The neighbor nodes observe $\theta = \{T, PDR\}$. Therefore, the power set can be represented as

$$2^{\theta} = \{\varphi, \{T\}, \{PDR\}, \{unknown\}\}$$

where

$$\{unknown\} = \{T\} \cup \{PDR\}$$

Given T and PDR, the basic probability assignments for nodes X, Y, and Z are as follows

$$m_T(X) = 0.7;\ m_T(Y) = 0.75;\ m_T(Z) = 0.65;\ m_T(U) = 0.1$$

$$m_{PDR}(X) = 0.75;\ m_{PDR}(Y) = 0.7;\ m_{PDR}(Z) = 0.75$$

Using equation (9), the observation by X, Y, and Z the combination becomes

$$m_{T,PDR}(X) = m_T(X) \oplus m_{PDR}(X) = 0.61$$
$$m_{T,PDR}(Y) = m_T(Y) \oplus m_{PDR}(Y) = 0.61$$
$$m_{T,PDR}(Z) = m_T(Z) \oplus m_{PDR}(Z) = 0.58$$

After the decision about the attacker is finalized, a method to find the location of the node is invoked. Complex numerical calculations are involved in location estimation in wireless networking. A complex calculation yields higher accuracy, but it requires a more powerful processor. Our goal is to reduce the complexity to estimate the compromised node's location with limited processor capability.

We have utilized the TDoA method for simplicity. In this method, normally at least three neighbor nodes send signals to the target node at different times. This is considered the most traditional methodology to find the location of the node.[18] To obtain TDoA measurements, the signal sources must lie on a hyperboloid by keeping a constant range difference with the measuring nodes. Assuming the master beacon node is B_1, then the distance from the transmitter to the ith beacon node is

$$R_i = \sqrt{(X_i - x)^2 - (Y_i - y)^2} \tag{10}$$

In a two-dimensional (2D) implementation, the target location can be estimated from two TDoA measurements based on the intersections of signals with the hyperbola created. Assuming that B_1, B_2, and B_3 are beacon nodes measuring the target, the intersection point calculated as a result is target point A. The process is shown in Figure 2.

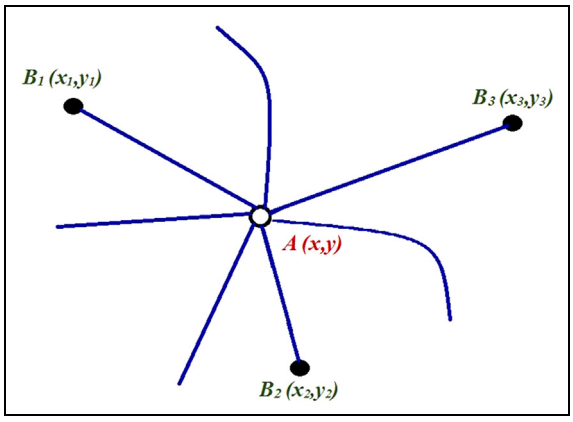

Figure 2. The location of the attacker.

In Figure 2, the three sensor nodes are B_i with the locations (x_i, y_i), where $i = 1$, 2, or 3 and $A = (x, y)$ is a point in plane. The difference in the range with the corresponding beacon nodes with respect to the beacon B_1, in which the transmitted signal arrives first, is

$$R_{i,1} = cd_{i,1} = R_i - R_1 \tag{11}$$

Here, c is the speed of signal propagation, $R_{i,1}$ is the difference in the range between the first beacon B_1 and the ith beacon ($B_1(i > 1)$), R_1 is the distance between the first beacon node and the transmitter, and $d_{i,1}$ is the estimate of TDoA corresponding to the first beacon B_1 and the beacon ($B_1(i > 1)$). A set of nonlinear hyperbolic equations is defined by this relationship. The solution of the set yields the 2D coordinates of the source.

The difficult task is to solve the nonlinear equation (11). Linearization of the set of equations is the common practice for these types of equations. One of several linearization processes is the Taylor series.[18,19] In Friedlander[20] and Schau and Robinson,[21] the authors present an alternative to the Taylor series expansion, which is to first transform the set of nonlinear equations into a different set. Rearranging the form of equation (11) into

$$R_{i,1}^2 = (R_{i.1} + R_1)^2 \tag{12}$$

And subtracting equation (10) at $i = 1$ from equation (12) results in

$$R_{i,1}^2 + 2R_{i,1}R_1 = X_i^2 + Y_i^2 - 2X_{i,1}x - 2Y_{i,1}y + x^2 + y^2 \tag{13}$$

Here, $X_{i;1}$ and $Y_{i;1}$ are equal to X_i–X_1 and Yi–Y_1, respectively. The set of equations in equation (13) are linear in the location of the source $A(x; y)$ and in the range of the first receiver of the source R_1 as the unknowns and are more easily handled.

To solve R_1, we employ Chan's method, a non-iterative resolution of the hyperbolic intersection point estimation problem. The method is capable of optimized performance for arbitrarily placed sensors. This solution is applicable in scenario of both distinct and closed sources. The errors in TDoA estimates are considered to be small, and this method works as an approximation to a maximum-likelihood estimator.

Following Chan and Ho's method[22] for the three beacon node system ($B = 3$) and generating two TDOAs, the solution of x and y can be found in terms of R_1 from equations (13). The solution is presented in the following form

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} X_{2,1} & Y_{2,1} \\ X_{3,1} & Y_{3,1} \end{bmatrix}^2 \times \left\{ \begin{bmatrix} R_{2,1} \\ R_{3,1} \end{bmatrix} R_1 + \frac{1}{2} \begin{bmatrix} R_{2,1}^2 - K_2 + K_1 \\ R_{3,1}^2 - K_3 + K_1 \end{bmatrix} \right\} \quad (14)$$

where

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

Substituting equation (14) into equation (10) with $i = 1$, a quadratic equation is formulated in terms of R1. Substitution of the positive root back into equation (8) yields the result. Hence, the system can detect the location point of the attacked node that basically $A(x; y)$. The position error can be determined using equation (15)

$$\Delta d = \sqrt{(x - x_0)^2 + (y - y_0)^2} \quad (15)$$

Results

As a simulation experiment, we performed a case study with sensors deployed randomly in a $b \times b$ square field. We used temperature measurement data as a physical parameter. We chose to use a Gaussian distribution for the temperature range, with zero mean and two sigma variations, analogous to the methodology adopted by Sentz and Ferson.[13] In the latter, they utilized one sigma variation for a stricter information set. We assumed adequate data sets to have stricter conditions (with perhaps two sigma variations), which can significantly increase the average accuracy. In our case, we took the average of the results of 20 runs. Our average result is from 95% (with one sigma variation) to 99.99% (with two sigma variations). The temperature varied from 8°C to 14°C in the information set we adopted.

Table 1. The simulation parameters.

Parameters	Values
Packet size	500 bytes
Initial energy	2 J
Transmission range	100 m
Routine protocol	AODV
Simulation time	1 min
Number of nodes	500

AODV: ad hoc on-demand distance vector.

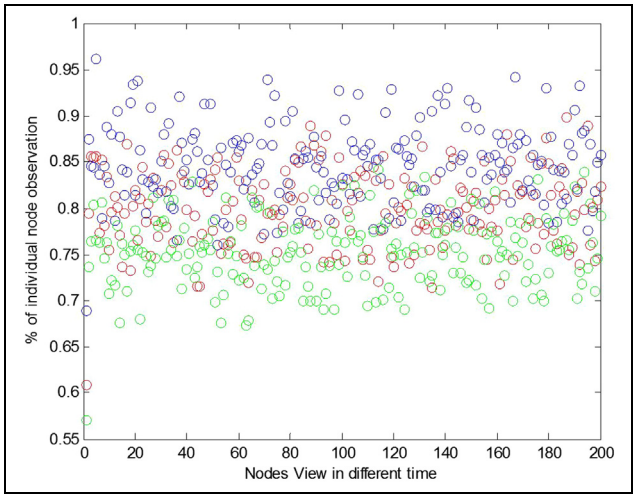

Figure 3. Observation of the nodes.

The simulation was designed and simulated in MATLAB. MATLAB R2015a version has been used to do the simulation. In order to set the simulation environment, we have created an area of 500 m by 500 m and we have set 500 randomly distributed nodes on that area. Additionally, we have created 25 nodes as an attacked node out of the existing nodes. DST has been implemented in order to find the attacker and TDoA for the location detection. We employed the DST of combination to do the simulation. We performed the DST simulation with individual pieces of evidence from the one-hop neighbor sensor nodes of the network. We assume that the system will not survive if 50% or more sensors are attacked or malicious node. In any active network, we can detect many attacker nodes if it is attacked. The simulation parameters are shown in Table 1. The simulation results are based on 200 different observations of the nodes.

In Figure 3, it is clearly seen that observation with three sensor nodes of X, Y, and Z are shown in blue, red, and green colors. The observation reaches almost the same conclusion about the attacker, that is, between 75% and 85% certainty that node A is an attacker.

Figure 4 shows the simulation results, which portrays the neighbor sensor nodes observations of the

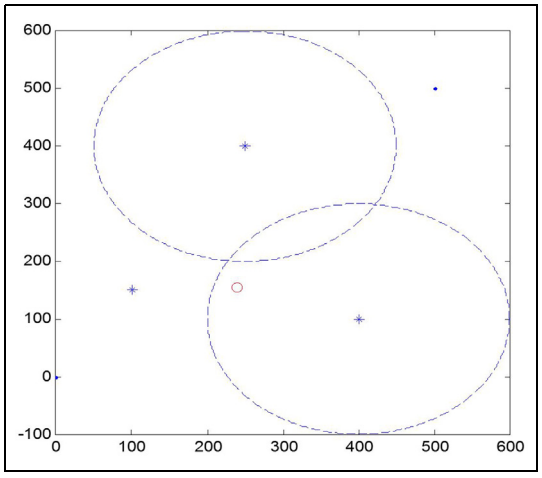

Figure 4. Location of the node.

suspected sensor node A. The observations by the one-hop neighbor nodes *X, Y*, and *Z* are also shown.

After the identification of attacker utilizing DST, we find the location of the node using TDoA method using equation (14). Figure 4 shows the location of the attacker node in red circle. The beacon nodes on blue star.

From the above results, it is obvious that the system was successfully working to conclude about the attacked node and find its locations. From the simulation result as shown in Figure 4, the exact location of the node is in red circle but we can see that there is slight position error of the exact location of the node.

Conclusion

Each country is trying to keep their border safe and secure to control the unwanted entry from their neighboring countries. Border monitoring systems are a distinctive domain of the smart technologies by the utilization of WSNs. WSNs itself have some constrain in terms of its security. Therefore, in order to implement WSN in the border, it is mandatory to have a secure WSN. In this article, we have investigated potential attacks in WSN systems and presented a solution for securing system against attack to be implemented in the border. In particular, we have developed a methodology to find location information of the attacker. To do this, we exploit multiple pieces of independent evidence and implemented DST to combine the multiple pieces of evidences for the attacker decision and to find the approximate location we have used TDoA methods. DST has the capability of modeling the independent uncertain event and TDoA has the simplicity which lead out system to the low latency and less computation. The simulation result shows that the algorithm works to find the attacked node and its approximate location. In future work, another detection algorithm will be incorporated to make the system more robust, resilient and to get the higher accuracy. Moreover, hardware of the complete system will be implemented and tested.

Acknowledgements

The authors acknowledge King Abdulaziz City for Science and Technology (KACST) in Saudi Arabia for sponsoring and supporting this work.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Ahmed M, Huang X, Sharma D, et al. Wireless sensor network internal attacker identification with multiple evidence by Dempster-Shafer theory. In: *Proceedings of the 12th international conference on algorithms and architectures for parallel processing,* volume part II, Fukuoka, Japan, 4–7 September 2012, pp.255–263. Berlin: Springer.
2. Ahmed M, Huang X and Cui H. Smart decision making for internal attacks in wireless sensor network. *Int J Comput Sci Netw Secur* 2012; 12(12): 15–23.
3. Ahmed M, Huang X and Sharma D. A taxonomy of internal attacks in wireless sensor network. *Int J Electr Comp Energ Electron Commun Eng* 2012; 6: 203–206.
4. McKitterick JB. Sensor deployment planning for unattended ground sensor networks. In: *Proceedings of SPIE 5417, unattended/unmanned ground ocean and air sensor technologies and applications VI*, Orlando, FL, 1 September 2004, p.382. Bellingham, WA: SPIE.
5. Li J and Ren Q. Compressing information of target tracking in wireless sensor networks. *Sci Res* 2011 3(2): 73–81.
6. Maharrey BK, Lim AS and Gao S. Interconnection between IP networks and wireless sensor networks. *Int J Distrib Sens Netw* 2012; 8: 1–15.
7. Staddon J, Balfanz D and Durfee G. Efficient tracing of failed nodes in sensor networks. In: *Proceedings of the 1st ACM international workshop on wireless sensor networks and applications*, Atlanta, GA, 28 September 2002, pp.122–130. New York: ACM.
8. Marti S, Giuli TJ, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks. In: *Proceedings of the 6th annual international conference on mobile computing and networking*, Boston, MA, 6–11 August 2000, pp.255–265. New York: ACM.
9. Zhang Y and Lee W. Intrusion detection in wireless adhoc networks. In: *Proceedings of the 6th annual*

international conference on mobile computing and networking, Boston, MA, 6–11 August 2000, pp.275–283. New York: ACM.
10. Znaidi W, Minier M and Ubéda S. Hierarchical node replication attacks detection in wireless sensor networks. In: *IEEE 20th international symposium on personal, indoor and mobile radio communications*, Tokyo, Japan, 13–16 September 2009. New York: IEEE.
11. Garofalo A, Sarno CD and Formicola V. Enhancing intrusion detection in wireless sensor networks through decision trees. In: Vieira M and Cunha JC (eds) *Dependable computing*. Berlin: Springer, 2013, pp.1–15.
12. Ahmed M and Mahmood AN. Novel approach for network traffic pattern analysis using clustering-based collective anomaly detection. *Ann Data Sci* 2015; 2(1): 111–130.
13. Sentz K and Ferson S. *Combination of evidence in Dempster-Shafer theory*. Sandia Report. SAND 2002-0835, April 2002. Binghamton, NY: Binghamton University.
14. Kay RU. Fundamentals of the Dempster-Shafer theory and its applications to system safety and reliability modelling. *Reliab Theor Appl* 2007; 3(4): 173–185.
15. Koks D. *An introduction to Bayesian and Dempster-Shafer data fusion*. Laverton Ave, ACT, Australia: DSTO Systems Sciences Laboratory, 2003.
16. Tabassian M, Ghaderi R and Ebrahimpour R. Combination of multiple diverse classifiers using belief functions for handling data with imperfect labels. *Expert Syst Appl* 2012; 39(2): 1698–1707.
17. Campos F and Cavalcante S. An extended approach for Dempster-Shafer theory. In: *IEEE International conference on information reuse and integration*, Las Vegas, NV, 27–29 October, pp.338–344. New York: IEEE.
18. Ahmed M, Huang X and Sharma D. A novel framework for abnormal behaviour identification and detection for wireless sensor networks. *Int J Comput Commun Eng* 2012; 6(2): 148–151.
19. Foy WH. Position-location solutions by Taylor-series estimation. *IEEE T Aerosp Electron Syst* 1976 12(2): 187–194.
20. Friedlander B. A passive localization algorithm and its accuracy analysis. *IEEE J Ocean Eng* 1987 12(1): 234–245.
21. Schau H and Robinson A. Passive source localization employing intersecting spherical surfaces from time-of-arrival differences. *IEEE T Acoust Speech* 1987; 35(8): 1223–1225.
22. Chan YT and Ho KC. A simple and efficient estimator for hyperbolic location. *IEEE T Signal Proces* 1994; 42(8): 1905–1915.