A NOVEL TWO-STAGE ALGORITHM PROTECTING INTERNAL ATTACK FROM WSNS

Muhammad Ahmed[1], Xu Huang[1]and Hongyan Cui[2]

[1]Faculty of Information Sciences and Engineering, University of Canberra, Australia
Muhammad.ahmed@Canberra.edu.au, xu.huang@canberra.edu.au
[2]SICE, Beijing University of Posts and Telecommunications, China
cuihy@bupt.edu.cn

ABSTRACT

Wireless sensor networks (WSNs) consists of small nodes with constrain capabilities. It enables numerous applications with distributed network infrastructure. With its nature and application scenario, security of WSN had drawn a great attention. In malicious environments for a functional WSN, security mechanisms are essential. Malicious or internal attacker has gained attention as the most challenging attacks to WSNs. Many works have been done to secure WSN from internal attacks but most of them relay on either training data set or predefined thresholds. It is a great challenge to find or gain knowledge about the Malicious. In this paper, we develop the algorithm in two stages. Initially, Abnormal Behaviour Identification Mechanism (ABIM) which uses cosine similarity. Finally, Dempster-Shafer theory (DST)is used. Which combine multiple evidences to identify the malicious or internal attacks in a WSN. In this method we do not need any predefined threshold or tanning data set of the nodes.

KEYWORDS

Wireless Sensor Network, Security, Internal Attack, Cosine similarity, Dempester-Shafer Theory

1. INTRODUCTION

Wireless sensor networks (WSNs) are a new technology for collecting data with autonomous sensors [1]. This technology is first motivated by military applications. As example battlefield surveillance, transportation monitoring, and sensing of nuclear, biological and chemical agents [2-5] is considered. Recently, this technology is widely used in our daily life because they are low cost, low power, rapid deployment, self-organization capability and cooperative data processing, such as habitat monitoring [6], intelligent agriculture, home automation [7], etc. A Typical WSN is shown in Figure1.

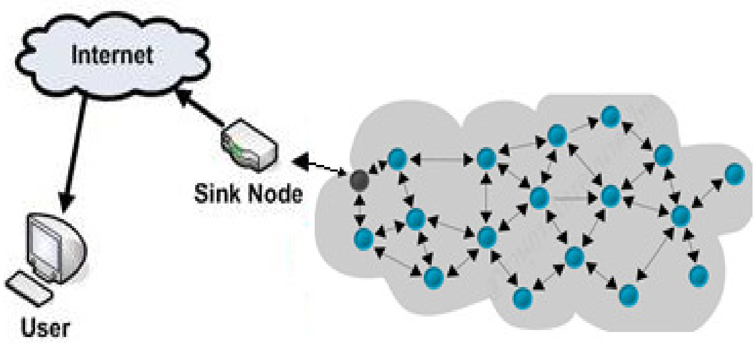

Figure1: A typical WSN

DOI : 10.5121/ijcnc.2013.5107

Extracting meaningful and actionable information from these applications, however, remains a challenge. According to the applications of WSN the node deployment strategy is decided. Normally, in WSN the environment is unknown, hostile, remote harsh fields, disaster are as toxic environment. Hence there is no standard deployment strategy exist. The deployment usually done by scatter by a possible way based the application scenario [6].

In all communication networks including WSN, security provisioning is a critical requirement. WSN has different characteristics compare to the conventional communication networks that includes open nature of wireless medium, unattended operation, limited energy, memory, computing power, communication bandwidth, and communication range which makes the WSN security mechanism tough. Even, it is more susceptible to the security attack in comparing to the traditional wired network. The security of WSN can be investigated in different viewpoints, following our paper [8] WSN attacks can be classified as two major categories: *external* and *internal* attacks according to the domain of attacks. External attack is defined as the attack does not belong to the network and it does not have any internal information about the network such as cryptographic information. When a legitimate node of the network acts abnormally or illicit way it is consider as a suspect of an internal attack. To perform the internal attack in the network it uses the compromised node, which definitely can destroy or disrupt the network. In this paper we focus on the internal attacks. The major internal attacks in WSN includes Denial of Service (DoS) attacks, information and selective forwarding, Wormhole attack, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding.

Considering the characteristics of WSN many algorithms have developed for the secure functionality of WSN. Many existing research has focused on the pair wise key establishment of the node for data exchange, authentication access control and defence against an attack. These works mainly focused on the traditional cryptographic information, data authentication in order to build the relationships among the sensors. But, the cryptographic methods sometimes are not very efficient and effective. The unreliable communications through wireless channel can make the communication technique vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary [9]. The compromised entity of the network appears as a legitimate node. So it is easy for the adversary to launch the internal attacks. When a node is attacked by a malicious the node will behave aberrantly. It will perform tampering the massage from other member; data drop or excessive data broadcasting.

Considering the existing work, in order to protect WSN in an efficient way more attention is necessary. Hence, in our research, we have proposed two-stage mechanism to find the internal attack in a targeted WSN. In order to do that we first check the transmission range based on individual regions. If the node is in the transmission range we use the cosine similarity method to find the abnormally behaved node based on the message frequency with *k*-means algorithm [10]. In the final stage to ensure about the internal attack we used Dempester- Shafer Theory (DST). As DST has the feature of dealing with uncertainty [11]. In the both stages the algorithm observes neighbour nodes parameters but the judgement is made based on DST. It considers the observed data as hypothesis. In the observation; it might be uncertain which hypothesis fits best. Therefore, DST makes it possible to model several single pieces of evidence within multi hypotheses relations [12]. In our proposed method the system does not need to have any prior knowledge of the pre-classified training data of the nodes.

The rest of the paper organizes as follows: section 3 presents the related works followed by the characteristics of WSN. A discussion about internal attack is presented in this section 4. The generic security requirements and vital security challenges is in section 5 and 6, respectively. Section 7 describes our network and the system architecture. The description of new algorithm, concept and implementation process how to detect internal attack is presented in Section 8.

Section 9 illustrates the simulation results. A brief discussion is given with our conclusion in Section 10.

2. RELATED WORK

Multi-hop communication is used in WSNs in order to increase the network capacity as in multi-hop routing; messages may traverse many hops before reaching their destinations. However, the deployed sensor nodes are normally physically unprotected to make the network cost effective. They are always deployed in open or hostile environments in a possible way. Hence, they can be easily captured and compromised by the adversary, and then it can easily extract sensitive information, control of the compromised nodes. So, those nodes end up by giving the service for the adversary. Therefore, when a node is compromised, an adversary gains access to the network and can produce malicious activities. The attacks are involved in different fashion such as corrupting network data or even disconnecting major part of the network.

The network layer attacks are discussed extensively by Karlof and Wagner in [13].They mentioned altered or replayed routing information and selective forwarding, node replication, Sybil attacks or black-grey-sink holes, and HELLO flooding. Other than that some papers even discussed several attacks in term of network's resiliency. In [14], the researchers discussed how to keep WSN routing protocols as stateless as possible to avoid the proliferation of specific attacks and provide for a degree of random behaviour to prevent the adversary from determining which the best nodes to compromise are. They defined three items, namely (i) average delivery ratio, (ii) average degree of nodes, and (iii) average path length to describe the networks resiliency. Obviously, the more efficient and effective ways are needed.

In [15] the authors addressed pollution attacks against network coding systems in wireless mesh networks. They proposed a lightweight scheme, DART that uses time-based authentication in combination with random liner transformations to defend against pollution attacks.

A few papers also address pollution attacks in internal flow coding systems use special crafted digital signatures [16-17] or hash functions [18-19]. Recently some papers discuss the preventing the internal attacks by related protocols [20, 21].

It is noted that resiliency of WSNs are related to the security of WSNs [22], where a definition of network resiliency was discussed based on the comparisons with other similar terminologies such as robustness etc. In this paper we follow the definition of [23], i.e. resiliency is the ability of a network to continue to operate in presence of k compromised nodes to present our definition of "resiliency degree" and an algorithm to control the compromised nodes with SDT in the targeted WSN. Here we automatically take the assumption that the attacks are from internal when we highlighted the nodes become "compromised nodes."

In cryptographic approaches, the source uses cryptographic techniques to create and send additional verification information that allows nodes to verify the validity of coded packets.

In terms of the attack model, synoptically speaking there are two types of international attacks, namely (i) exceptional message attack, by which the attacks will tamper the message content or generate fake messages and (ii) abnormal behaviour attacks, by which the transmission will be abnormally changed such as dropping the messages, forwarding the message to a particular receivers, broadcasting redundant or meaningless messages to increasing the traffic load in the network, etc. As we are focusing on the controllable resiliency based on the internal attackers we shall focus on the case abnormal attributes and some of cases (i) can be extended to what we discussed in this paper.

3. CHARACTERISTICS OF WSN

WSN is currently used for real-world unattended physical environment to measure numerous parameters. So, the characteristics of WSN must be considered for efficient deployment of the network. The significant characteristics of WSN are described as follows [24]:

Low cost: Normally hundreds or thousands of sensor nodes are deployed to measure any physical environment in WSN. In order to reduce the overall cost of the whole network the cost of the sensor node must be kept as low as possible.

Energy efficient: Energy in WSN is used for different purposes such as computation, communication and storage. Sensor node consumes more energy compare to any other for communication. If they run out of the power they often become invalid as we do not have any option to recharge. So, the protocols and algorithm development should consider the power consumption in the design phase.

Computational power: Normally the node has limited computational capabilities as the cost and energy need to be considered.

Communication Capabilities: WSN typically communicate using radio waves over a wireless channel. It has the property of communicating in short range, with narrow and dynamic bandwidth. The communication channel can be either bidirectional or unidirectional. With the unattended and hostile operational environment it is difficult to run WSN smoothly. So, the hardware and software for communication must have to consider the robustness, security and resiliency.

Security and Privacy: Individual sensor node should have adequate security mechanisms in order to avoid illegal access, attacks, and accidental damage of the information inside of the sensor node. Furthermore, additional privacy mechanisms must also be included.

Distributed sensing and processing: The large number of sensor node is distributed uniformly or randomly. In WSNs, each node is capable of collecting, sorting, processing, aggregating and sending the data to the sink. Therefore the distributed sensing provides the robustness of the system.

Dynamic network topology: In general WSNs are dynamic network. The sensor node can fail for battery exhaustion or other circumstances, communication channel can be disrupted as well as the additional sensor node may be added to the network that result the frequent changes in the network topology. Thus, the WSN nodes have to be embedded with the function of reconfiguration, self-adjustment.

Self-organization: The sensor nodes in the network must have the capability of organizing themselves as the sensor nodes are deployed in an unknown fashion in an unattended and hostile environment. The sensor nodes have work in collaboration to adjust themselves to the distributed algorithm and form the network automatically.

Multi-hop communication: A large number of sensor nodes are deployed in WSN. So, the feasible way to communicate with the sinker or base station is to take the help of an intermediate node through routing path. If one node needs to communicate with the other node or base station which is beyond its radio distance it must be through the multi-hop route by intermediate nodes.

Application oriented: WSN is different from the conventional network due to its nature. It is highly dependent on the application ranges from military, environmental as well as health sector. The nodes are deployed randomly and spanned depending on the type of use.

Robust Operations: Since the sensors are going to be deployed over a large enough to cover the required area and sometimes hostile environment. Hence, the sensor nodes have to be fault and error tolerant. Therefore, sensor nodes need the ability to self-test, self-calibrate, and self-repair

Small physical size: Sensor nodes are generally small in size with the restricted range. Due to its size its energy is limited which makes the communication capability low.

4. INTERNAL ATTACKS OF WSN

In the manufacturing process the cost-effectiveness of the sensor nodes is considered. In most application of WSN the sensor nodes are usually not even physically well protected. Considering the characteristics of WSNs it can easily be summarised that WSN is very easy to be attacked internally. An adversary can easily corrupt the network by gaining the internal information of the node. The attacks are involved in corrupting network data or even disconnecting major part of the network. Following our previous paper [8] we have described the major internal attacks as follows.

Denial of Service (DoS) attacks: DoS attack is an explicit attempt to prevent the authentic user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to genuine traffic. As a result, the user can not get the access to the desired service or system. The basic types of attack involved: Jamming, Tapering, collision, Homing, flooding, etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming.

Wormhole attack: Just like the theoretical wormholes in space, this attacker can send packets, routing information, ACK etc., through a link outside the network to another node somewhere else in the same network. This way an attacker can fool nodes into thinking they are neighbours, when they are actually in different parts of the network. This can also confuse routing mechanisms that rely on knowing distances between nodes. A wormhole attack can be used as a base for eaves dropping, not forwarding packets in a DOS like manner, alter information in packets before forwarding them etc.

Sinkhole attack: This is a DOS attack, where a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a “low cost route first “protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths. The neighbours of this node will also chose this node in routes, and compete for the bandwidth. This way the malicious node creates a black hole inside the network.

Sybil attack: The Sybil attack targets fault tolerant schemes such as distributed storage, disparity, multipath routing and topology maintenance. This is done by having a malicious node present multiple identities to the network. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.

Selective forwarding attack: In this attack, malicious nodes can decide not to forward packets of certain types or to from certain nodes. Even though the protocol is completely resistant to the sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch this type of attack if it is strategically located near the source or a base station.

Spoofing attack: In this attack, a malicious node may be able to create routing loops, wormholes, black holes, partition the network and etc., by spoofing, altering or replaying routing information.

Hello flood attack: Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbours. A node receiving such a packet may assume that it is within the radio range of the sender but this assumption may be false.

Flooding attack: In this attack, a malicious node may send continuous connection requests to a victim node effectively flooding the victim's network link.

In network coding intermediate nodes actively mix or code input packets and forward the resulting coded packets. The very nature of packet mixing also subjects network coding systems to a severe security threat, knows as a pollution attack, where attackers inject corrupted packets into the network. Since intermediate nodes forward packets coded from their received packets, as long as least one of the input packets is corrupted, all output packets forwarded by the node will be corrupted. This will further affect other nodes and result in the epidemic propagation of the attack in the network. In [14], it addressed pollution attacks against network coding systems in wireless mesh networks.

5. Generic Security Requirements of WSN

The nature of a WSN leads a challenge to provide full security to the network. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. In order to provide the complete security in a WSN all message have to be encrypted and authenticated. An adversary can use natural impairments to modify the original message or information as well as can make the information unavailable because of WSN nature and uncontrolled environments. Security requirements in a WSN are similar to the wireless ad hoc network [8, 25].

WSNs have the general security requirements of data confidentiality, authentication, integrity, freshness and secure management.

Confidentiality: An adversary can choose any node to eavesdrop as long as it is within the radio range as the signals are transmitted over the wireless channel. So, it is a threat for the data confidentiality as the attacker can gain the cryptographic information.

Authentication: To determine the legitimate node and whether the received data has come from the authorized node or not authentication is important.

Integrity: Information moving through the network could be altered. So integrity is important to trust the received information from the network.

Freshness: To save the network from the replay packets it is important to ensure that the received data is fresh and unused.

Secure management: It is important to manage the distribution of cryptographic keying material in the network.

6. Vital Challenges of WSN Security

A WSN has three major properties that made the security mechanism challenging.

a. Resource Constraints

b. Operational Environment, and

c. Wireless Multihop Communication.

It is commonly assumed that sensor nodes are highly resource constrained; e.g., the resources are comparable to the Berkeley MICA2 motes and TMote mini is presented in the Table 1 Thus, security protocols for WSNs must be executable on the available hardware and especially must be very efficient in terms of energy consumption and execution time.

Table1: Existing Sensor Platform [26], [27]

Characteristics	Mica2	TMote mini
RAM (Kbytes)	4	10
Program Flesh Memory (Kbytes)	128	48
Maximum data rate (Kbps)	76.8	250
Power Draw: Receive (mW)	36.81	57
Power Draw: Transmit (mW)	87.90	57
Power Draw: sleep (mW)	0.048	0.003

The operational environment of most WSNs is assumed to be unattended or even hostile. Since sensor nodes are usually not assumed to be physically protected by some tamper-resistant hardware, an adversary is able to compromise sensor nodes. Thus, even if security mechanisms, such as node-based authentication, are deployed, an adversary is able to participate in the network since the adversary has access to all data [14], e.g., cryptographic keys stored on the node. Thus, security protocols must be able to operate even if sensor nodes are compromised.

The wireless communication enables an adversary to eavesdrop, inject, drop, or alter messages or to perform denial of service (DoS) attacks by jamming the wireless channel. In contrast to most other wireless networks, the communication is performed in a multihop way. This introduces additional challenges. Compromised nodes may be part of a route, enabling them to modify forwarded messages, or a compromised node injects a large amount of false messages to drain the energy resources of all forwarding nodes.

7. Network and System Architecture

A network with *N* uniformly distributed sensor nodes over the area of $N_x \times N_y$ with self-organized *m* clusters into squared field in a 2D scenario. Sensing nodes are responsible to collect and forward the monitored data around them. Then, the collected data sent to the sinker. In order to detect the abnormal behaviour of the sensor nodes we use ABIM and DST mechanism if it is within the transmission range. We will consider the system is synchronized.

In addition, as a case study, for a temperature measurement we will consider that the sensor deployed area with temperature varying from 8 degree to 14 degree in °C. Based on the Gaussian distribution, within 2 sigma (standard deviation) we will accept the temperatures. According to Holder et al [28], the choice of sigma value depends on the data set. 95.46% of the sensor data will fall within 2 standard deviation of the mean with 2 sigma consideration. The sampling rate is set to 0.1 Hz means 6 massages in a minute.

We will consider the temperature reading is normal or the node is behaving normally, if we find that the reading match withour sigma value and with the one hop neighbours. If the outcome from ABIM is abnormal node we will go ahead for the second stage implementation with DST. In DST we will check both physical (temperature) and transmission packet drop rate (PDR) parameter of the node.

Our temperature measurement in WSN system is based on a single sinker with randomly distributed static node. We assume the neighbour node with one hop will observe the data of the suspected internal attacker. Observed physical parameter (temperature) and transmission behaviour (packet drop rate) is considered as independent events. The observation of the events becomes the pieces of evidences. In the decision making process with Dempster-Shafer Theory we will combine the independent pieces of evidences.

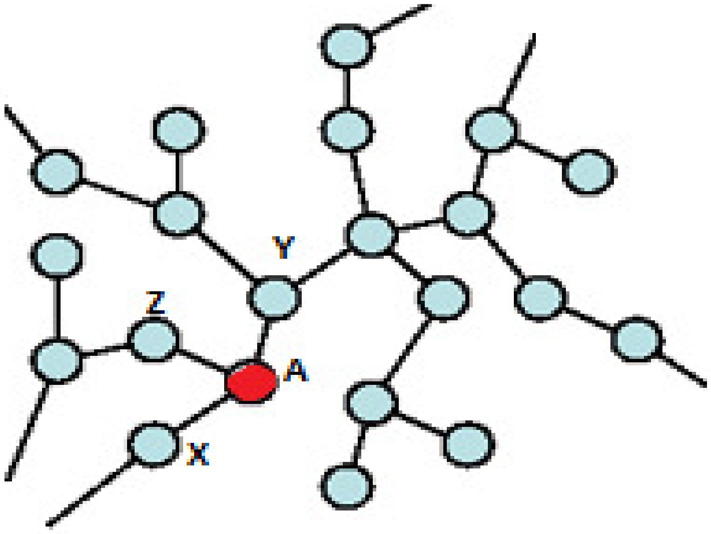

Figure 2: Three neighbour observing the attacker with one hop

Let's take the above scenario described in Figure 2, the neighbour nodes X ,Y and Z will observe the suspected internal attacker node A for its temperature (T) and packet drop rate (PDR). Before we go further discussion for Figure 2, we need to brief the ABIM and DST to present our novel algorithm, which will described in section five. Then we shall apply our designed algorithm to Figure 2 as study case for our initiative.

8. NETWORK MODEL AND DESIGNED METHOD

The system under consideration consists of an area of interest where region wise detection requirements are provided by the end user. We model the area of interest as a grid Ω of N_x× N_y points. The ratio of the detection to miss requirements at every point on the grid are ordered in two N_xN_y × 1 vector of the ratio of the probability, p_d/ p_m. There are two common sensing models found in literature, binary detection model and the exponential detection model. Both models share the assumption that the detection capability of a sensor depends on the distance between the sensor and the phenomena, or target to be detected. Following [4] notations we have the case that for the binary detection model, the probability of detection p_d (t,s) is given as:

$$p_d(t,s) = \begin{cases} 1 & \text{if } d(t,s) \le r_d \\ 0 & \text{if } d(t,s) > r_d \end{cases} \tag{1}$$

wherer_d is the detection radius and $d(t,s)$ is the distance between the target's position "t" and the sensor location "s" on a plane. The exponential model is a more realistic model, where the probability of detection corresponds to

$$p_d(t,s) = \begin{cases} e^{-\alpha d(t,s)} & \text{if } d(t,s) \le r_d \\ 0 & \text{if } d(t,s) > r_d \end{cases} \tag{2}$$

whereα is a decay parameter that is related to the quality of a sensor or the surrounding environment. In the exponential model of equation (2), even if a target is within the detection radius, there is a probability that it will not be detected, which means it will be missed. As this model is closer to the realistic case, we shall use this model.

The process of linking individual sensors' detection characteristic to the overall probability of detection requirements on the grid is mathematically quantified using miss probabilities, p_{miss} = 1 −p_d, where p_d is the probability of detection. The overall miss probability $M(x, y)$ corresponds to the probability that a target at point (x, y) will be missed by all sensors, which is

$$M(x,y) = \prod_{(i,j)\in\Omega} p_{miss}((x,y),(i,j))^{u(i,j)} \tag{3}$$

where $u(i,j)$ represents the presence or absence of a sensor at the location (i, j) on the grid, and corresponds to

$$u(i,j) = \begin{cases} 1, & \text{if there is a sensor at } (i,j) \\ 0, & \text{if there is no sensor at } (i,j) \end{cases} \tag{4}$$

Taking the natural logarithm of the both sides in equation (3), we have

$$m(x,y) = \sum_{(i,j)\in\Omega} u(i,j) \ln p_{miss}((x,y),(i,j)) \tag{5}$$

where $m(x, y)$ is so-called the overall logarithmic miss probability at the point (x, y). Thus we have the function $b(x, y)$ as

$$b(x, y) = \begin{cases} \ln p_{miss}((x, y), (0,0), & d((x, y), (0,0) \leq r_d \\ 0, & d((x, y), (0,0)) > r_d \end{cases} \tag{6}$$

The overall logarithmic miss probabilities for all points on the grid can be arranged in a vector m of dimension $N_x N_y \times 1$ that corresponds to equation (7) as shown below:

$$\mathbf{m} = [m(x, y), \forall (x, y) \in \Omega]^T$$

$$\mathbf{u} = [u(i, j), \forall (i, j) \in \Omega]^T$$

and $\mathbf{m} = \mathbf{Bu}$ (7)

The $((i\text{-}1)N_y + j)$-th element of u indicates the number of sensors deployed at point (i, j) on the grid. The matrix **B** is of dimension $N_x N_y \times N_x N_y$, and it contains

$$\{b(x - i, y - j), \forall (x, y) \in \Omega, (i, j) \in \Omega\}$$

$b(x–i, y–j)$ corresponds to the (r, c)-th entry of **B**, where $r = (x–1)N_y + y$ and $c = (i–1)N_y + j$.

Essentially, $b(x–i, y–j)$ quantifies the effect of placing a sensor at the point (i, j) on the logarithmic miss probability at the point (x, y) on the grid. If there are some compromised nodes distributed in a WSN, how those compromised nodes could be detected by their so-called abnormal attributes among the network, such as irregular change of hop count that implicates sinkhole attacks; the signal power is impractically increasing which may indicate wormhole attacks; abnormally dropping rate traffic behaviours related the related nodes most likely to be compromised, etc.

In the initial stage we have designed ABIM that is sensitive to the abnormal event. In the conventional cryptographic way it is not possible to detect the internal attacker because of the unpredictable wireless channel. The unreliable channel makes it easy to compromise the node and establish untrustworthy relationship [29]. The attacker always behaves abnormally, so it is mandatory to identify the misbehaved node to secure the network.

WSN is densely deployed and continuously observe the phenomenon, this characteristics drive WSN node normally encounter the spatial-temporal correlation. In our research we considered the message generated from the nodes is similar for a defined period with the sampling rate if 0.1Hz (1 message per 10 second). Considering the limited storage of the sensor we store minimum information of the Message in S. The message m_i is consists of the content of the representative message (∂) and frequency of the message (α). $m_i = \langle \partial_i, \alpha_i \rangle$, The set of the message is shown in the equation (8)

$$S = \{m_1, m_2, m_3, ...m_n\} \tag{8}$$

It is the set that will store the latest message that is sent to the network recently. When a new message m_{new} is sent it arrives at the cluster head which can be authenticated by the similarity function with *S*. The difference between the detected and average temperature is divergence. If we denote $D^i(m_{new})$ as the divergence between the new and the normal message we have the set as equation (9) [12].

$$D^i(m_{new}) = \{D^1(m_{new})D^2(m_{new}).....D^m(m_{new})\} \tag{9}$$

where,

$$D^i(m_{new}) = \left| m_{|M|} - m_{new} \right|$$

Based on equation (8) if the data is different from the content considering the Gaussian distribution of temperature and the threshold than it is new message. The threshold is defined as the mean of the data set. If $D^i(m_{new})$ is not within the threshold it is considered as new message. For further authentication we will use the cosine similarity with frequency consideration. If we consider new message frequency ω , the cosine similarity is in equation (10).

$$COSIM = \frac{\alpha.\omega}{\|\alpha\|\|\omega\|} \tag{10}$$

If the two frequencies are similar it is considered as normal message otherwise it is considered as false message and the node will be considered as abnormal node.

```
Algorithm 1

I. Get $m_{new}$

For $i$ = 1 to $|M|$

If $MinTh \le D^i(m_{new}) \ge MaxTh$

printf “Good Node”

   else go to II

II. for $i$ = 1 to $T$

Execute the equation (10)

      If COSIM $i \le 0.6$

printf “the node is an internal attacker”

      else

        Go to step I

end
```

In the simulation we set the sampling rate 0.1Hz from the 6 minutes observed imperial data and our case study we have the calculation for the consign similarity for a one hop neighbour with the abnormally behaved node.

α = {6 5 6 5 6 4}

ω= {1 0 3 2 1 5}

Cosine Similarity (COSIM) = 36 / (13.19) *(6.32)

= 36 / 83.42

= 0.43

With the decision of ABIM decision we further implement Dempester-shafer theory (DST). In DST, probability is replaced by an uncertainty interval bounded by belief and plausibility. Belief is the lower bound of the interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents the non-refuting evidence [30]. In this reasoning system, all possible mutually exclusive hypothesis (or events) of the same kind are enumerated in the frame of discernment also known as universal discloser θ . A basic belief assignment (BBA) or mass function is a function m: 2^{θ} → [0, 1], and it satisfies two following condition

$$m(\phi) = 0 \tag{11}$$

$$\sum_{A \subseteq \theta} m(A_j) = 1 \tag{12}$$

In which ϕ is the empty set and a BBA that satisfy the condition $m(\phi) = 0$. The basic probability number can be translated as *m*(*A*) because the portion of total belief assigned to hypothesis A, which reflects the evidences strength of support. The assignment of belief function maps each hypothesis B to a value*bel* (*B*) between 0 and 1. This defined as

$$bel(B) = \sum_{j: A_j \subseteq A} m(A_j) \tag{13}$$

The upper bound of the confidence interval is the plausibility function, which accounts for all the observations that do not rule out the given proposition. It maps each hypothesis *B* to a value *pls* (*B*) between 0 and 1, can be defined as follows.

$$pls(B) = \sum_{j: A_j \cap B \neq \phi} m(A_j) \tag{14}$$

The plausibility function is a weight of evidence which is non-refuting to *B*. equation (15) shows the relation between belief and plausibility.

$$pls(B) = 1 - bel(\sim B) \tag{15}$$

The hypothesis not *B* is representing by ~*B*. The functions basic probability numbers, belief and plausibility are in one-to-one correspondence and by knowing one of them, the other two functions could be derived [31]. Figure 3 shows the graphical representation of the above defined measures belief and plausibility.

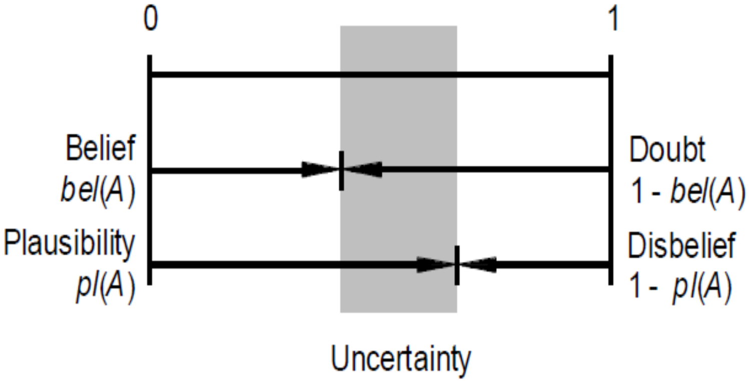

Figure 3: Measure of belief and plausibility

Assuming m1(A) and m2(A) are two basic probability number by two independent items of evidence means two independent neighbour node which act as observers in the same frame of discernment. The observations (the pieces of evidence) can be combined using Dempster's rule of combination (known as orthogonal sum) as in equation (16).

$$(m_1 \oplus m_2)(B) = \frac{\sum_{i,j:A_i \cap A_j = B} m_1(A_i) m_2(A_j)}{1 - \sum_{i,j:A_i \cap A_j = \phi} m_1(A_i) m_2(A_j)} \qquad (16)$$

where $\oplus$ represents the Dempster's combination operator that combines two basic probability assignments or basic belief assignments (BBA) into the third [17]. To normalize the equation we consider L is a normalization constant defined by the equation (17), More than two belief function can be combined with pairwise in any order.

$$L = \frac{1}{K} \qquad (17)$$

where ,

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

The combination rule assigns the belief according to the degree of conflict between the evidences and assigns the remaining belief to the environment and not to common hypothesis. It makes possible to combine with most of their belief assigned to the disjoint hypothesis without the side effect of a counterintuitive behaviour. Belief resembles the certainty factors or evidences [18]. The conflict between two belief functions bel_1andbel_2, denoted by the $Con(bel_1, bel_2)$ is given by the logarithm of normalization constant [19] shown in equation (18)

$$Con(bel_1, bel_2) = \log(L) \qquad (18)$$

If there is no conflict between the $bel_1$and bel_2 than $Con(bel_1, bel_2) = 0$ and if there is nothing in common between two evidences $Con(bel_1, bel_2) = \infty$ [20]. The DST automatically incorporates the uncertainty coming from the conflicting evidences. Following the reference [20] we can come up with a Dempester-shafer combination, which can be given as in equation (19)

$$m(B) = (m_1 \oplus m_2)(B) = \frac{L \sum_{i,j:A_i \cap A_j = B} m_1(A_i)\, m_2(A_j)}{1 + \log(L)} \qquad (19)$$

In order to find the internal attacks in our case we can execute the above framework with equation (19). The algorithm used to do the simulation is shown below. The temperature threshold ∂_T and ∂_{PDR} is the threshold for the packet drop rate which is set based on the training data.

```
Algorithm 2

I. Get the view of the neighbor node view
Input: $m_T$ , $m_{PDR}$ , $\partial_T$ ,$\partial_{PDR}$
$m_T[\ ]$\\ BPA assignment
$m_{PDR}[\ ]$\\ BPA assignment
II. Execute the equation (9)
$m_{T,PDR}[\ ]$\\
        If $m(B) < 0.6$
    Output result accepted
printf “the node is an internal attacker”
    else
      Go to step I
end
```

DST application in our system works by considering the independent event as temperature T and PDR as described in section 4. Our case the universal discloser or the set of local element can be observed by the one hop neighbouris $\theta = \{T, PDR\}$. Hence the power set becomes

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

Where,

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

In our specific case study and in simulation we have the imperial data as below. The observation of node*A* by nodes*X*, *Y* and *Z*

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

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

Using the equation (19) the observation by X , Y and Z the combination becomes,

$$m_{T,PDR}(X) = m_T(X) \oplus m_{PDR}(X)$$

$$m_{T,PDR}(Y) = m_T(Y) \oplus m_{PDR}(Y)$$

$$m_{T,PDR}(Z) = m_T(Z) \oplus m_{PDR}(Z)$$

9. Results and Simulations

Temperature measurement is considered in our experimental work with randomly deployed WSN. For the temperature range we have considered Gaussian distribution mean with 2 sigma similar to the approach taken by holder *et al.* [10], even though in holder experiment he used 1 sigma for the constrain of data set but we assume we have sufficient data set to choose 2 sigma. In the simulation environment the parameter we have set is shown as follows,

Table 2: The Parameters

Parameters	Values
Packet Size	500 bytes
Initial Energy	2 J
Packet Size	500 bytes
Regional Area	(0,0) to (500,500)

The experiment was done in the MATLAB environment. In the deployed sensor field area we have set the temperature range 8 to 14 degree centigrade. Gaussian distribution is used for the mean and data threshold for ABIM with the training data. In the DST implementation we have simulated 200 different observations by the neighbour nodes.

The abnormal behaviour of the node was identified according to the methodology of ABIM which is described in section 5. Figure 4 shows the randomly distributed sensor filed and the detected abnormal node in red (node 16). The value was set 29 degree to make node 16 as a suspected node for the simulation purpose.

With the abnormal node detection of ABIM we farther implement Dempester-shafer Theory (DST). Figure 5 describe the observation about the node A. it shows the observation by node X (node 2), Y (node 7) and Z (node 12). from the figure it is clearly seen that three nodes observation gives the common result between 75 % to 85% that the node A (Node 16) is compromised or an internal attacker.

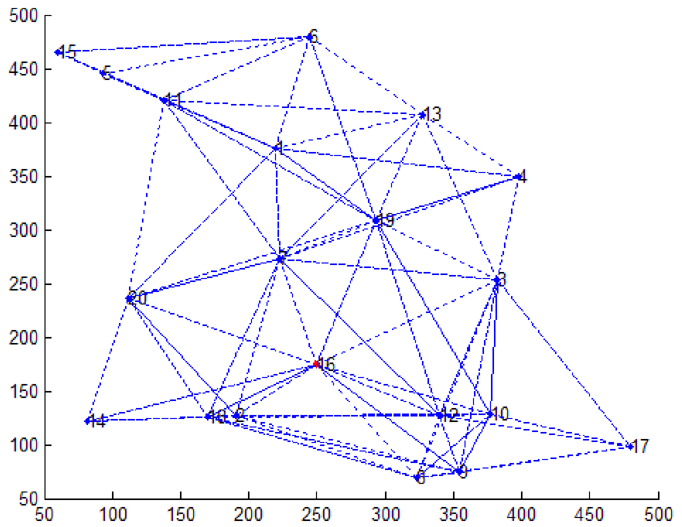

Figure 4. Sensor field

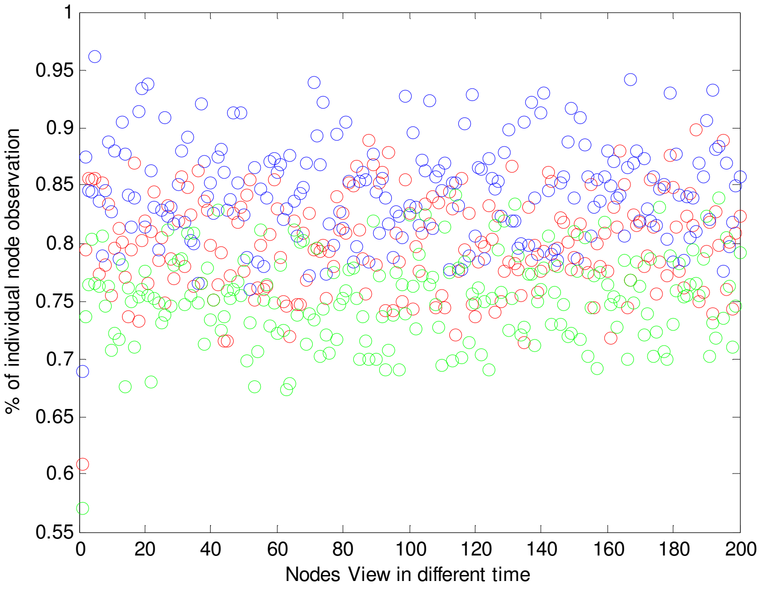

Figure 5.Observation of node *A* by *X*,*Y*,and *Z*in Figure 2.

10. CONCLUSION

We have carefully investigated internal attacks for WSN and create a novel algorithm for protecting WSNs from the internal attacks based on evaluation using ABIM and DST with our case study, temperature measurements in this paper. We first illustrate the method to identify the compromised nodes by the abnormal attributes. Internal attacker always mismatch with the normal behaviour of the node in different both in physical and transmission parameters. With the neighbour normal node evaluation using DST we have identified the internal attack in Wireless Sensor Networks. The simulation results, shows different observation and DST combination result for identified internal attacker.

In future, we would like to implement the algorithm in the hardware level to test in real time environment.

ACKNOWLEDGEMENT

One of authors would like to thank the works has been partly supported by National Natural Science Foundation of China (Grant No. 61201153), the National 973 Program of China under Grant (Grant No. 2012CB315805), and the National Key Science and Technology Project (Grant No. 2010ZX03004-002-02).

REFERENCES

[1] Huang X, Ahmed M, Sharma D, “Timing Control for Protecting from Internal Attacks in Wireless Sensor Networks”, *IEEE, ICOIN 2012*, Bali, Indonesia, February 2012.

[2] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets”, IEEE Signal Processing Mag., vol. 19, pp. 17-29, Mar 2002.

[3] C. Meesookho, S. Narayanan and C. Raghavendra, “Collaborative classification applications in sensor networks”, Proc. of Second IEEE Multichannel and Sensor array signal processing workshop, Arlington, VA, 2002.

[4] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, B. Krogh, “An energy-efficient surveillance system using wireless sensor networks”, MobiSys'04, Boston, MA, 2004.

[5] B. Sinopoli, C. Sharp, L. Schenato, S. Shaffert, Sh. S. Sastry, “Distributed control applications within sensor networks”, Proc. Of the IEEE, August 2003.

[6] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop-Hurley, "Wireless ad hoc sensor and actuator networks on the farm," 2006, pp. 492-499.

[7] Z. Feng, "Wireless sensor networks: a new computing platform for tomorrow's Internet," 2004, pp. I-27 Vol.1.

[8] Ahmed M., Hunag X., Sharma D., “A Taxonomy of Internal Attacks in Wireless Sensor Network”, *ICIS 2012*, Kuala Lumpur, Malaysia 2012.

[9] Ahmed M., Hunag X., Sharma D., “A Novel Framework for Abnormal Behaviour Identification and Detection for Wireless Sensor Networks”, *ICIS 2012*, Kuala Lumpur, Malaysia 2012.

[10] Shakhnarovish G., Darrell T., Indyk P., “ Nearest-neighbor meathods in learning na d vision”, (MIT press 2005)

[11] Khalaja F., Khalajb M., Khalaj A.H., “Bounded Error for Robust Fault Detection under Uncertainty, Part 1: Proposed Model Using Dempster-Shafer Theory”, Journal of Basic and Applied Scientific Research 2012, 2(2)1233-1240, ISSN 2090-4304 (2012)

[12] Auden J, “ A logic for uncertain Probabilities”, international journal of uncertainity, Fuzziness and Knowledge-Based Systems, Vol. 9, No. 3, June 2001.

[13] C. Karlof and D. Wagner, “Secure routing inn wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, Vol. 1 no. 2-3, pp. 293-315, August 2003.

[14] Ochirkhand Erdene Ochir, Marine Minier, Fabrice Valois, and Apostolos Kountouris, “Resiliency of Wireless Sensor Networks: Definitions and Analyses”, 2010 17th International Conference on Telecommunications, pp828-835.

[15] Jing Dong, Reza Curtmola, and Cristina Nita Rotaru, “Parctical Defenses Against Pollution Attacks in Intra-Flow Network Coding for Wireless Mesh Networks,” WiSec’09, March 16-18, 2009, zurich, Switzerland, pp111-122.

[16] D. Charles, K. Jain, and K. Lauter, “Signatures for network coding,” 40th Annual Conference on Information Sciences and Systems, 2006.

[17] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, “An efficient signature-based scheme for securing network coding against pollutions attacks,” in Proc. Of INFOCOM OS , Phoenix, AZ, April, 2008.

[18] M. Krohn, M. Freedman, and D. Mazierres, “On-the-fly verification of rateless erasure codes for efficient content distribution,” Security and Privacy, 2004. Proc. 2004 IEEE Symposium on, pp.226-240, 9-12 May 2004.

[19] C. Gkantsdis and P. Rodriguez, “ Cooperative security for network coding file distribution,” Proc. Of INFOCOM 2006.

[20] Ahmad Ababnah, Balasubramaniam Naatarajan, “Optimal control based strategy for sensor deployment.” IEEE Tran. On Systems, Man, and cybernetics, Part A: Systems and Humans, vol. 41, no. 1 Jan. 2011.

[21] Ahmed Sobeih, Jennifer C Hou, Lu-Chuan Kung, Ning Li, Honghai Zhang, Wei Peng Chen, Hung-Ying Tyan, Sun Yat-Sen and Hyuk Lim, “J-Sim: A simulation and emulation environment for wireless sensor networks,” IEEE Wireless Communications, August 2006, pp104-119.

[22] Xu Huang, Muhammad Ahmed, and Dharmendra Sharma, “A Novel Algorithm for Protecting from Internal Attacks of Wireless Sensor Networks” 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing , Melbourne, Oct 24-26, 2011.

[23] Ochirkhand Erdene-Ochir, Marine Mibier, Fabrice Valois and Apostolos Kountouris, “Resiliency of wireless sensor networks: definitions and analyses,” 2010 17th International Conference on Telecommunications. Pp-828-835.

[24] C. Buratti , A. Conti , D. Dardari and R, Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution” , Sensors 2009, ISSN 1424-8220, pp 6869-6896, 2009.

[25] K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647.

[26] https://www.eol.ucar.edu/rtf/facilities/isa/internal/CrossBow/DataSheets /mica2.pdf, accessed on November 24, 2011.

[27] http://sentilla.com/files/pdf/eol/Tmote_Mini_Datasheet.pdf, accessed on November 24, 2011.

[28] C. Holder, R. Boyles, P. Robinson, S. Raman, and G. Fishel, “Calculating a daily Normal temperature range that reflects daily temperature variability”, American Meteorological Society, June 2006.

[29] 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.

[30] K. Sentz, “Combination of Evidence in Dempester-Shafer Theory”, System Science and Engineering Department, Binghamton University, SAND 2002-0835, April 2002.

[31] U. Rakowsky, “Fundamentals of the Dempster-Shafer theory and its applications to system safety and reliability modelling” *RTA # 3-4, 2007*, December – Special Issue.

[32] D. Koks, S. Challa, “An Introduction to Bayesian and Dempster-Shafer Data Fusion” , *Published by DSTO Systems Sciences Laboratory, Australia, November 2005.*

[33] M. Tabassian, R. Ghaderi, R. Ebrahimpour, “Combination of multiple diverse classifiers using belief functions for handling data with imperfect labels” *Expert Systems with Applications 39, Elsevier 2011.*

[34] F. Campos, S. Cavalcante, “An Extended Approach for Dempster-Shafer Theory” *Information Reuse and Integration, 2003. IRI 2003. IEEE 2003.*

Authors

Muhammad Raisuddin Ahmed currently serves as Lecturer (Teaching Fellow) at the Faculty of Information Sciences and Engineering, University of Canberra (UC), Australia. He was a distinguished member of the Board of directors of ITE&E Canberra Division, Engineers Australia in 2011. Besides, from March 2009 until July 2011, he was working as a Research officer and Project coordinator of BushLAN project at the Plasma research Laboratory, Research School of Physics and Engineering, at the Australian National University (ANU), Australia. During this time he was also an academic in the College of engineering and computer science at ANU from February 2010 till November 2011. He is pursuing his PhD at the UC, Australia. He has received Master of Engineering studies in Telecommunication and a Masters of Engineering Management degree from the University of Technology, Sydney (UTS), Australia. He obtained his Bachelor of Engineering (Hons) Electronics Majoring in Telecommunications degree from Multimedia University (MMU), Malaysia. His Research interest includes: Wireless Sensor Networks, Distributed Wireless Communication, Blind Source Separation, RF technologies, RFID implementation.

Professor (Dr) Xu Huang has received the B.E. and M.E. degrees and Ph.D. in Electrical Engineering and Optical Engineering prior to 1989 and the second Ph.D. in Experimental Physics in the University of New South Wales, Australia in 1992. He has earned the Graduate Certificate in Higher Education in 2004 at the University of Canberra, Australia. He has been working on the areas of the telecommunications, cognitive radio, networking engineering, wireless communications, optical communications, and digital signal processing more than 30 years. Currently he is the Head of the Engineering at the Faculty of Information Sciences and Engineering, University of Canberra, Australia. He is the Course Conveners “Doctor of Philosophy,” “Masters of Information Sciences (by research),” and “Master of Engineering.” He has been a senior member of IEEE in Electronics and in Computer Society since 1989 and a Fellow of Institution of Engineering Australian (FIEAust), Chartered Professional Engineering (CPEng), a Member of Australian Institute of Physics. He is a member of the Executive Committee of the Australian and New Zealand Association for Engineering Education, a member of Committee of the Institution of Engineering Australia at Canberra Branch. Professor Huang is Committee Panel Member for various IEEE International Conferences such as IEEE IC3PP, IEEE NSS, etc. and he has published about two hundred papers in high level of the IEEE and other Journals and international conference; he has been awarded 9 patents in Australia.

A/Prof.Hongyan Cui has received the Ph.D. in School of Telecommunications Engineering in Beijing University of Posts and Telecommunications in 2006. She is engaged in communication network research and development work since 2000. She has been participated in two National 973 Projects, four 863 Projects, two National Nature Funds, a ministerial project, and a corporate-funded research project. She has published over 30 papers in the important journals / conferences, two books since 2003. She applied eight patents. She is the reviewer of the " Chinese Journal of Electronics"," Journal of Communications " ,"Journal of Beijing University of Posts and Telecommunications", "IEEE Networks Magazine SI", "Chaos" etc. She has trained 34 undergraduate students for graduation design,, and guided 31 Masters, in which 16 have graduated , and now she also assisting guided 3 doctoral students. Her research interest is future networks architecture, ESN, and Clustering.