Peer Trust based Trust and Reputation Model for Wireless Sensor Networks to Protect Border

Mohammed Aseeri†, Muhammad R Ahmed†, Ahmed Al Ghamdind†† and Sultan AlMorqi†††

†Faculty of Information Sciences and Engineering, University of Canberra, Australia
††Ministry of Interior, Border Guard, Kingdom of Saudi Arabia
†††King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia

Summary
Border security has become a high-priority issue in many countries around the world. The Conventional border surveillance or petrol systems consist of check points and border troops but it does not provide the complete security. In addition to that smart fencing is a solution to extend the eyes and ears of the Border Patrol. The idea is to use wireless sensor network (WSN) which consists of low-cost and multifunctional resources constrain autonomous nodes. WSN is used to create a virtual fence consisting of a large number of heterogeneous devices such as cameras, sensors, and mobile stations, providing continuous security monitoring, which is a cost effective. In order to function wireless sensor network efficiently security and trust model is a vital challenge. In this paper we focuses on peer trust based trust and reputation system management, which is an innovative solution for maintaining a minimum security level between two entities having transactions or interactions within a distributed system.

Key words:
Wireless Sensor Network (WSN), Border Security, Peer Trust, Security

1. Introduction

Recently, technological advances in the design of processors, memory and radio communications have propelled an active interest in the area of distributed sensor networking, in which a number of independent, self-sustainable nodes collaborate to perform information gathering and processing in real time. Networks of such devices are commonly referred to as Wireless Sensor Networks (WSNs). Wireless sensor networks are a new technology for collecting data with autonomous sensors[1]. It is first motivated by military applications such as battlefield surveillance, transportation monitoring, and sensing of nuclear, biological and chemical agents [2]. Recently, this technology became more popular because of its cost effectiveness and our daily life applications such as habitat monitoring, intelligent agriculture, and home automation. It consists of large number of low cost, low power and multifunctional sensors embedded with short range wireless communication capability[3]. The data is transmitted to the sink in an autonomous way which has high capacity of storage and analysis power. According to the applications the deployment strategy is decided. When the environment is unknown or hostile such as remote harsh fields, disaster are as toxic environment the deployment usually done by scatter by a possible way, sometimes by small an aircraft. Thus the position of the sensor nodes may not be known in advance. In the post deployment the sensor nodes perform self-organization mechanism to set up the network by determining the neighbor and setting up the routing table by themselves in an autonomous way. A typical WSN is shown in Figure 1.

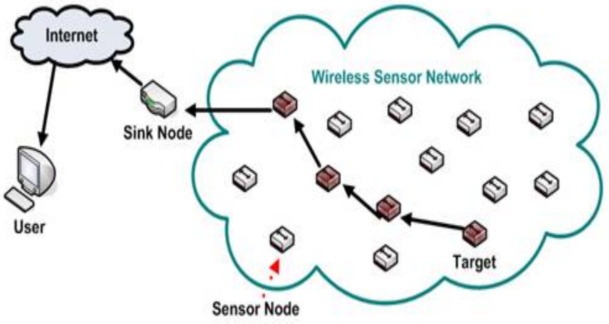

Fig. 1 A Typical WSN

Security provisioning is a critical requirement for any communication network. Security in the wireless sensor network is challenging and important task because of its characteristics that includes, open nature of wireless medium, unattended operation, limited energy, memory, computing power, communication bandwidth, and communication range [4]. So, it is more susceptible to the security attack compare to the traditional wired network as well as wireless ad hoc network.

Although WSN shares many properties with Wireless ad hoc network and may require similar techniques such as routing protocols but in certain cases it directly prohibit using the protocols proposed in wireless ad hoc network. Thus, the characteristics and architecture differs as well. To demonstrate this issue, the dissimilarities between the WSN and wireless ad hoc network are summarized [5]:

Manuscript received August 5, 2014
Manuscript revised August 20, 2014

• The number of sensor nodes (hundreds or thousands nodes) in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network.
• Sensor nodes are densely deployed, so multiple sensors can perform to measure the same or similar physical phenomenon.
• Sensor nodes are prone to failures because of battery exhaustion and hostile environment.
• The topology of a sensor network changes very frequently caused by node failure.
• Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are based on point-to-point communications.
• Sensor nodes are limited in power, computational capacities, and memory.
• Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

The unique properties and characteristics of WSN need to be considered in order to secure the WSN. Many algorithms have developed for the secure functionality of WSN. Most of the work has focused on the pair wise key establishment, authentication access control and defense against attack. Most importantly those works mainly focused on the traditional cryptographic information, data authentication in order to build the relationship between the sensors. However, the unreliable communications through wireless channel made the communication technique vulnerable by allowing the sensor nodes to compromise and release the security information to the adversary. The compromised entity of the network acts as a legitimate node. So it is easy for the adversary to perform the internal attacks. When internal attack occurs for a node, this node will behave abnormally such as tampering the massage from other member, dropping the data or broadcast excessive data.

Our Research focuses on trust and reputation system management, which is an innovative solution for maintaining a minimum security level between two entities having transactions or interactions within a distributed system. The main goal of this security approach is to distinguish the benevolent sensor from malicious sensors in the network. A trust and reputation model is generally composed of five components: gathering information, scoring and ranking, selecting entities, having transaction, as well as giving reward or punishment. We studied and present simulation result Peer Trust model in this paper.

Peer Trust system [6], a dynamic peer-to-peer trust and reputation model, initially aims at estimating and evaluating the trustworthiness, or goodness, of a peer in an environment. It identifies five factors related to trust and reputation management for computing the trustworthiness value of a given peer, namely:

1. The feedback a peer retrieves from others;
2. The feedback scope, or field (number of transactions);
3. The credibility factors of the source;
4. The transaction context factor addressing the criticalness of transactions; as well as
5. The community context factors interpreting related characteristic.

The rest of the paper is organized as follows: section 2 presents the protocols of WSNs followed by section 3. In section 4 Existing Hardware Platform followed by the related works to secure the border in section 5. Section 6 consists of the common attacker model in the border. Section 7 we present our trust and reputation model. The results are shown in section 8 and the conclusion in section 9.

2. Protocols of WSNs

WSNs are designed to carry out various tasks which are underpinned by several protocols. In this section, we are going to discuss some major related protocols for WSNs. Routing protocols of WSNs are inspired by ad hoc networking for some similarities in their characteristics [7]. Moreover, WSNs have some specific properties such as coverage cast traffic profile, strong energy constrain, densely deployed high number of nodes [8][9]. Thus, we need to take special care for WSNs. There are different ways we can classify the sensor networks routing protocols. According to Ochirkhand [8], the classification of routing protocol can be divided into four categories: Flooding based routing, Probabilistic routing, Location based routing and Hierarchical routing, as shown in the Figure 2.

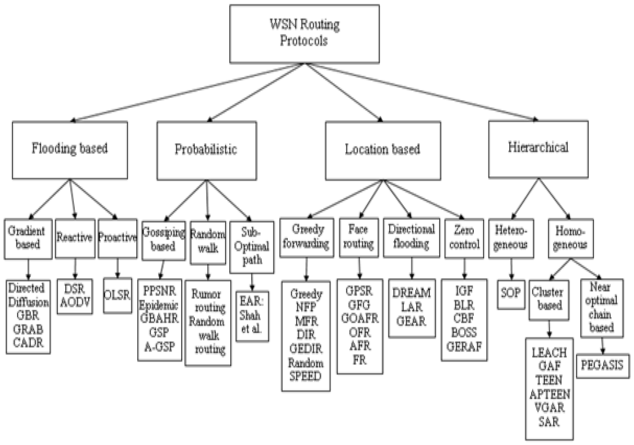

Fig. 2 Routing protocols of WSNs

Flooding based routing is a static algorithm which uses flooding mechanism to discover routs. In flooding based protocol every incoming packet is sent out on every outgoing line except the one it arrived on [10]. Flooding based generates infinite number of duplicate packets unless some measures are taken to damp the process. Probabilistic routing chooses the next hope using a dynamically assigned probability or random choice making their behaviour non-deterministic [8]. The location based routing protocols uses geographical location information to guide routing discovery and maintenance as well as data forwarding, enabling directional transmission of the information and avoiding information flooding in the entire network [11][12]. Each node need to know its destination, its own location and the location of the neighbour. Hierarchical routing are based on hierarchy among the nodes [8]. When larger amount of resources necessary to take care or routing table becomes enormous and makes routing impossible. The idea of hierarchical routing that suggests that routers should be divided into regions, with each router knowing all the details about how to route packets within its own region, but knowing nothing about the internal structure of other regions. Most of the routing protocol is shown in Figure 2. We list few popular routing protocols for wireless sensor networks as bellow [13]:

- Direct diffusion
- GBR (Gradient Based Routing)
- AODV (Ad hoc On-Demand Distance Vector)
- GPSR (Greedy Perimeter Stateless Routing)
- LEACH (Low Energy Adaptive Clustering Hierarchy)

3. Applications of WSNs

The August 1999 Business Week has identified WSNs as one of the most important technologies for various applications in 21st century [14]. It can be deployed on the ground, in the air, under water, on bodies, in vehicles, and inside buildings to measure different phenomenon based on the sensor nodes classifications. The existing applications can be categorised under some main general headings based on the sensor taxonomies [15] as follows:

- Military applications (e.g. Battlefield monitoring, Border surveillance)
- Environmental monitoring (e.g. Animal tracking, Flood detection)
- Commercial or human centric applications (e.g. Vehicle tracking, Patient monitoring)
- Robotics (e.g. Monitoring equipment and automation)

To get the maximum efficiency from any application and security sensor node selection is important. In the next section we have introduce the existing hardware platform for sensor nodes.

4. Existing Hardware Platform

There are numbers of hardware platform existed for WSNs. The experts from Commonwealth Scientific and Industrial Research Organisation (CSIRO) found that the best performance of a sensor network comes from adapting the nodes and communication methods to the local environment and the application [16]. We have listed a few main prototype and commercial motes/sensor nodes available in the market to choose from, which help us to select the hardware of WSNs in order to develop effective security mechanism as:

- BTnode (use Atmel ATmega 128L Microcontroller)
- Mica (use ATmega 103 Microcontroller)
- T-mote (use Texas Instruments MSP430 Microcontroller)
- IMote (use ARM core 12 MHz Microcontroller)

5. Related Work

In various contexts trust has been studied for long. It has started in the social science as an improvement topic. To build e commerce systems such as eBay the effect of trust has been analyzed [17]. For the online retailers in online systems Game theory and reinforcement learning are also used to model the reputation. In addition, trust management systems have been used for knowledge management and sharing over the internet as well as peer to peer and ad hoc networks[18].

In WSNs, most current trust research focuses on sensor radio communication [19]. Sensor nodes build reputation through wireless radio transaction with neighboring nodes, and routing decisions are made based on the trust level of the sensor nodes.

In [20], Ganeriwal, Balzano and Srivastava proposed RFSN which is a reputation- based framework for high integrity WSNs. In their method Bayesian formulation is utilized to update reputation metrics with new transaction, density-based outlier detection discovers data outliers, and an aging mechanism is used against the sleeper attack.

Agent based trust model has been studied by Chen et al. [21] , in their proposed framework they develop a distributed agent-based trust management scheme. The agent node use watchdog mechanism to observe the behaviour of the sensor nodes and computes the trust and rating for them. There is other researcher as well studied agent based systems such as Boukerche and Li in [22] introduced ATRM for system design point of view. The ATRM is based on a clustered WSN with backbone and on a mobile agent system; it introduces a trust and reputation local management strategy with the help from the mobile agent running on each node.

Study on the effects of rating algorithms by Liang and Shi in [23]. In their research they looked at the uncertainty.

They first, study the effect of all factors based on a simple averaging rating algorithm in terms of several proposed performance metrics. Then they compare different rating aggregation algorithms in the same context and platform, focusing on several relevant metrics.

6. Model of Attacks in Border

Information collected from WSNs is crucial in making border surveillance decisions; thus the most critical requirement for the WSNs design is to maintain a high level of security. The enemies are likely to hack the networks in order to eavesdrop or modify fetched data. They may also simply just physically destroy sensor nodes. As a result, protection should be applied against both physical attackers and malicious nodes [24].

The attacker's goal is to stop the monitoring network from detecting the border crossing event. This can be done in the following two ways:

First, the attacker can stop the sensor that senses the border crossing event from sending out any packet. As shown in the Figure 1, the intruder jams the channel of all sensors close to the border crossing path.

Second, the attacker can physically destroy or jam the channel of the base station and camera nodes to stop further analysis on suspicious areas. As a result, the system will not be able to notice any intrusion event in the field nor track the intruder's location.

7. Trust and Reputation System

An innovative solution for continuing a minimum security level between two bodies having communications or connections within a distributed system is Trust and reputation system management. Trust [25] is a precise level of the subjective probability with which an agent will accomplish a specific action; while a reputation [26] is anticipation about an agent's behavior based on information about it or opinions of its past behavior. In most cases, these two terms are not distinguished explicitly and could be used interchangeably.

The main goals of a trust and reputation system could be defined as follows [17]:

1. Collect and provide information that enable client nodes to discriminate benevolent server nodes and malicious server nodes;
2. Encourage nodes to be trustworthy;
3. Discourage untrustworthy nodes to participate in transactions.

A trust and reputation model is generally composed of five components [27][28]:

1. Gathering information,
2. Scoring and ranking,
3. Selecting entities,
4. Having transaction, and
5. Giving reward or punishment.

Gathering information: it is considered as the first component of a trust and reputation system, and it is in charge for gathering behavioral information about other entities or nodes, for example, peers, agents, of paths. The information collected might come from difference sources Error! Reference source not found.. It could be first-hand meaning direct observation or own experience, or second-hand meaning that the information provided by peers.

Once evidence about an entity has been properly collected and weighed, a reputation score is then calculated and given base on certain algorithm. The primary objective of this procedure is to provide the clients a measurable approach to decide which server node is most trustworthy.

In the next step a client selects the most trustworthy or reputable server entity in the community providing certain service and then effectively has an interaction with it. After receiving the service provided, the client will access the result and give a score of satisfaction.

According to the fulfillment obtained, the last step, punishing or rewarding, is carried out. If a server node is disastrous in making the client satisfied with the service provide, its reputation score will suffer, and the client is less likely to have transaction with it again.

The uniqueness of the Peer Trust system is the identification and application of the five parameters. This section introduces the general trust matric which combines the five parameters to compute the values of trustworthiness for a given sensor peer. In a given WSN, the trust value of a peer u could be computed via equation 1.

$$T(u) = \alpha \cdot \sum_{i=1}^{I(u)} S(u,i) \cdot CR(p(u,i)) \cdot TF(u,i) + \beta \cdot CF(u) \qquad (1)$$

where:

- $T(u)$: denotes the value of trustworthiness of peer u.
- α : denotes the weight factor for the collective evaluation, a weighted average of amount of satisfaction that peer u receives;
- β : denotes the weight factor for the community context factor.
- $I(u)$: denotes the total number of transactions that peer u has had with all other peers.
- $S(u,i)$: denotes the normalized the amount of satisfaction which peer u receives in its ith transaction.

There are existing reputation-based mechanisms that simply apply a binary reputation mechanism to evaluate the degree of satisfaction, in which 0 represents unsatisfied, while 1 represent satisfied. But according to the paper Error! Reference source not found. this evaluating system may not function well since in this way malicious node may hide its misbehavior via increasing its transaction volume. Taking that into consideration, a normalized the amount of satisfaction value is applied, where $S(u,i) = \frac{S(u,i)_{Binary}}{I(u)}$, where $S(u,i)_{Binary}$ represent the binary satisfaction (0 or 1) peer u received in its ith transaction.

$CR(p(u,i))$ denotes the credibility of the feedback that peer u receives from the i th peer ($p(u,i)$) it has transaction with. The reason why credibility of the feedback is important is that a peer may make false statements for other peers. For instance, a malicious sensor may give low satisfaction for a benevolent sensor, or give high satisfaction for a malicious sensor. As a result, a credibility of feedback should be introduced; and feedback with higher credibility should be weighed more when computing the trustworthiness of a give peer. Two mechanisms evaluating the credibility of feedback have been introduced.

Equation 2 exemplifies the initial mechanism, and the matric using this one to measure credibility of feedback is called T_{TVM} (where TVM stands for Trust Value Measurement). This mechanism uses the trust value of peer $p(u,i)$ to evaluate the trustworthiness of feedback received from it to peer u.

$$CR(p(u,i)) = \frac{T(p(u,i))}{\sum_{i=1}^{I(u)} T(p(u,i))} \qquad (2)$$

Equation 3 present a personalized similarity measurement (PSM) to rate the credibility of peer (u,i), and the matric using this one to measure credibility of feedback is called T_{PSM}. If we use w to represents the client sensor which wants to test whether u is trustworthy, then $Sim(p(u,i),w)$ is used to measures the personalized similarity between peer w and peer (u,i). This is computed via equation 0, where $IJS(p(u,i).w)$ is the common set of peers which peer w and peer $p(u,i)$ have had transaction with in the past, and x denotes a peer belonging to the set of peers; $\overline{IJS(p(u,\imath),w)}$ denotes the two vectors of feedback by peer w and peer $p(u,i)$; and $(\frac{\sum_{i=1}^{I(x,p(u,i))} S(x,p(u,i))}{I(x,p(u,i))} - \frac{\sum_{i=1}^{I(x,w)} S(x,w)}{I(x,w)})^2$ denote the standard deviation of the two feedback vectors.

$$CR(p(u,i),w) = \frac{Sim(p(u,i),w)}{\sum_{j=1}^{I(u)} Sim(p(u,i),w)} \qquad (3)$$

$$Sim(p(u,i),u) = -\sqrt{\sum_{(x \in IJS(p(u,i).u)} \frac{(\frac{\sum_{i=1}^{I(x,p(u,i))} S(x,p(u,i))}{I(x,v)} - \frac{\sum_{i=1}^{I(x,u)} S(x,u)}{I(x,u)})^2}{|\overline{IJS(p(u,\imath),u)}|}} \qquad (4)$$

$TF(u,i)$ denotes the transaction context factor of peer u's ith transaction. This is another importance factor since each transaction may differ from one another. Transaction contexts including size or category can have influence on the $TF(u,i)$ value.

Finally, $CF(u)$ denotes the community context factor which could be applied to address some community-specific issues, for instance, incentive problem Error! Reference source not found..

Typical Peer Trust Model implementation strategies include: trust data management, trust matric computation, as well as trustworthy peer selection.

Figure 3 is a scheme of the system architecture of Peer Trust system. Note that no central database is used; and all trust data are maintained across the peer-to-peer network in a distributed approach. Each system for a peer has a trust manager in charge of submitting feedback and evaluating trust, a tiny database storing global trust data, as well as a data locator responsible for placing and locating trust data.

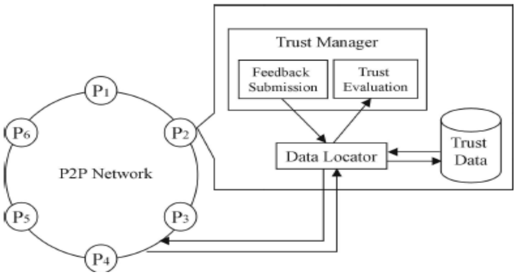

Fig. 3 A scheme of the system architecture of Peer Trust system.

Trust computing is done by the trust evaluation component according to the trust and reputation data. Previously discussed trust matric are applied at this stage. Two strategies are widely conducted: dynamic trust computation (DTC), where fresh data is used; as well as approximate trust computation (ATC), where cache is used to accelerate.

Algorithm:

```
find a server sensor $u$ providing services.
get a set of sensors which have had transactions sensor $s$
  before ($p(u,1)$, $p(u,2)$, … , $peer(u,I)$).
while $p(u,i) \in (p(u,1), p(u,2), \dots, p(u,I)$ do
    get the satisfaction value that $s$ receives from
  sensor $p(u,i)$, $S(u,i)$.
    get a set of sensors which have had transactions
  with sensor $p(u,i)$ and the client sensor $w$
    previously, $IJS(p(u,i).w)$ ($x_1$, $x_2$, …).
    while sensor $x_i \in IJS(p(u,i).w)$ do
        compute $S(x_i, p(u,i))$.
        compute $S(x_i, w)$.
    compute $S(x, p(u,i))$.
        compute $S(x, w)$.
        compute $Sim(p(u,i), w)$.
        compute $CR(p(u,i)$
    compute trust value of peer $u$, $T(u)$.
```

8. Results

A trust and reputation system with high performance should provide higher level of, better efficiency and easiness in finding trustworthy sensors, as well as lower level of energy consumption. However, there are always trade-offs among these three factors. For instances, a trust and reputation system providing high level of security might need to consume more energy to test and evaluate potential server sensors. Thus, we do not focus on a single character, but the overall performance in balancing these three factors to evaluate a trust and reputation system.
In our simulation we used TRMSim, the simulator randomly create WSN for experiments according this template as in Figure 4. Table 1 is the WSN parameters for this experiment:

Table 1: WSN parameter Settings

Network Parameters	
% Clients	15%
%Relay Servers	5%
Radio Range	10
Min. Num. of Nodes	200
Max. Num. of Nodes	200
Num. of Network	500
Num. of Execution	100

We used the idea of accuracy to evaluate the reliability and level of security delivered by the trust and reputation system. For a WSN applying a confident type of trust and reputation system to search for trustworthy sensors, The accuracy of a trust and reputation system is characterized by the percentage that the number of times when it successful selects trustworthy sensors (the former situation) out of the total number of transactions. For example, if a client sensor have transaction with different server sensors for 100 times, and it is satisfied with 99 transactions, and receive one bad services, it is considered that this trust and reputation system successfully selects trustworthy nodes for 99 times and fails once. Thus, the accuracy is 99% as shown in Figure 5.

The decreasing trend of accuracy in finding malicious sensors is more obvious; especially when the percentage of malicious sensor is higher than 70%, the accuracy sharply drops from 96% to 67%. This is because that the trust value of a sensor is determined by the evaluation it received from other sensors in its previous transactions. Malicious sensors might attack the network by giving low satisfaction to trustworthy sensors, or giving high average hops leading to the most trustworthy sensors

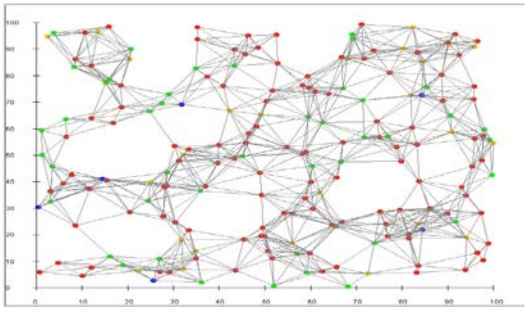

Fig. 4 Sensor field in the border

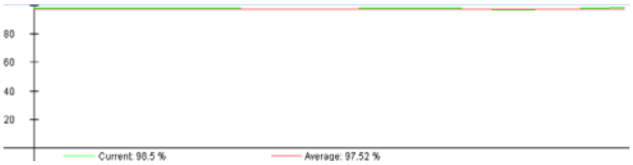

Fig. 5 Accuracy graph

which are selected by the client in a WSN applying a certain type of trust and reputation system. In a network applying Peer Trust system, a client needs to travel 6.4

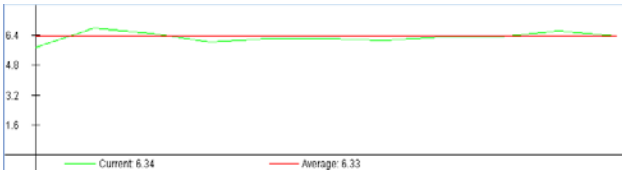

Fig. 6 Path length

Energy consumption of the network is the overall energy consumed in:
1. Client nodes sending request messages;
2. Server nodes sending response services;
3. Energy consumed by malicious nodes which provide bad services;
4. Relay nodes which do not provide services; and
5. The energy to execute the trustworthy sensor searching process of a certain trust and reputation system.

Figure 7 shows energy consumption which is measured in µJ.

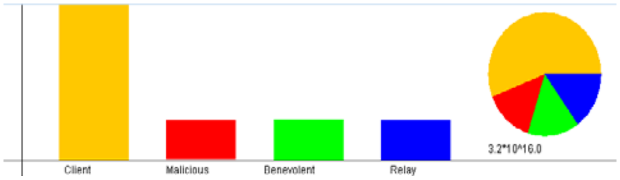

Fig. 7 Energy consumption

9. Conclusion

A Border protection is a typical domain for deployment of wireless sensor networks. As the end users are interested in the sensor data, the WSN must need to deliver the data with confidentiality. In this paper, we present analysis of possible attacks in border and peer trust based trust and reputation model to get the data in a secure manner. The simulation result is resented in the result section. For future improvement we are working on combining with other methods.

References

[1] M. Ahmed, X. Huang, and H. Cui, “Smart Decision Making for Internal Attacks in Wireless Sensor Network,” Int. J. Comput. Sci. Netw. Secur., vol. 12, no. 12, pp. 15–23, Dec. 2012.

[2] M. R. Ahmed, X. Huang, and H. Cui, “Mrakov Chain Monte Carlo Based Internal Attack Evaluation for Wireless Sensor Network,” Int. J. Comput. Sci. Netw. Secur., vol. 13, no. 3, pp. 23–31, Mar. 2013.

[3] M. R. Ahmed, X. Huang, and D. Sharma, “Protecting WSN from Insider Attack by Misbehaviour Judgement,” in Eighth International Conference on Wireless Communication and Sensor Network, Naresuan University, Phitsanulok, Thailand, 2012.

[4] M. R. Ahmed, X. Huang, H. Cui, and N. K. Srinath, “A novel two-stage Multi-crieteria evaluation for internal attack in WSN,” in 2013 13th International Symposium on Communications and Information Technologies (ISCIT), 2013, pp. 198–203.

[5] M. Ahmed, X. Huang, D. Sharma, and H. Cui, “Wireless Sensor Network: Cherecterestics and Architectures,” in World Academy of Science, Engineering and Technology, Penang, Malaysia, 2012, vol. 72, pp. 660–663.

[6] L. Xiong and L. Liu, “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” IEEE Trans Knowl Data Eng, vol. 16, no. 7, pp. 843–857, Jul. 2004.

[7] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, “Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey,” IEEE Commun. Surv. Tutor., vol. 15, no. 2, pp. 551–591, 2013.

[8] O. Erdene-Ochir, M. Minier, F. Valois, and A. Kountouris, “Resiliency of wireless sensor networks: Definitions and analyses,” in 2010 IEEE 17th International Conference on Telecommunications (ICT), 2010, pp. 828 –835.

[9] N. Rathi, J. Saraswat, and P. P. Bhattacharya, “A review on routing protocols for application in wireless sensor networks,” Int. J. Distrib. Parallel Syst. IJDPS, vol. 3, no. 5, pp. 39–58, Oct. 2012.

[10] S. Misra, S. C. Misra, and I. Woungang, Guide to wireless sensor networks. London: Springer, 2009.

[11] M. Al-Rabayah and R. Malaney, “A New Hybrid Location-Based Ad Hoc Routing Protocol,” in 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1–6.

[12] Z. Kai, T. Libiao, and L. Wenjun, “Location-Based Routing Algorithms for Wireless Sensor Network,” ZTE Commun., vol. 1, no. 1, pp. 1–9, 2009.

[13] Z. Manap, B. M. Ali, C. K. Ng, N. K. Noordin, and A. Sali, “A Review on Hierarchical Routing Protocols for Wireless Sensor Networks,” Wirel. Pers. Commun., vol. 72, no. 2, pp. 1077–1104, Sep. 2013.

[14] N. Gross, “21 ideas for the 21st century,” Business Week, pp. 78–167, 30-Aug-1999.

[15] M. El Brak and M. Essaaidi, “Wireless sensor network in home automation network and smart grid,” in 2012 International Conference on Complex Systems (ICCS), 2012, pp. 1–6.

[16] CSIRO, “Wireless sensor networks: a new instrument for observing our world.” [Online]. Available: http://www.csiro.au/Outcomes/ICT-and-Services/National-Challenges/Sensors-and-network-technologies.aspx. [Accessed: 30-Sep-2013].

[17] P. Resnick and R. Zeckhauser, “Trust among strangers in Internet transactions: Empirical analysis of eBay’s reputation system,” Adv. Appl. Microecon. Res. Annu., vol. 11, pp. 127–157, 2002.

[18] T. Tran and R. Cohen, “A Reputation–Oriented Reinforcement Learning Strategy for Agents in Electronic Marketplaces,” Comput. Intell., vol. 18, no. 4, pp. 550–565, Nov. 2002.

[19] M. Ahmed, X. Huang, D. Sharma, and L. Shutao, “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, Berlin, Heidelberg, 2012, pp. 255–263.

[20] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based Framework for High Integrity Sensor Networks,” ACM Trans Sen Netw, vol. 4, no. 3, pp. 15:1–15:37, Jun. 2008.

[21] H. Chen, H. Wu, J. Hu, and C. Gao, “Agent-Based Trust Management Model for Wireless Sensor Networks,” in International Conference on Multimedia and Ubiquitous Engineering, 2008. MUE 2008, 2008, pp. 150–154.

[22] A. Boukerche and X. Li, “An agent-based trust and reputation management scheme for wireless sensor networks,” in IEEE Global Telecommunications Conference, 2005. GLOBECOM ’05, 2005, vol. 3, p. 5 pp.–.

[23] Z. Liang and W. Shi, “Analysis of Ratings on Trust Inference in Open Environments,” Perform Eval, vol. 65, no. 2, pp. 99–128, Feb. 2008.

[24] A. G. Ahmed, M. Aseeri, and M. R. Ahmed, “A Novel Trust and Reputation Model Based WSN Technology to Secure Border Surveillance,” vol. 2, no. 3, pp. 263 – 265, Jun. 2013.

[25] D. Collard, “Review of Trust: Making and Breaking Cooperative Relations by Diego Gambetta,” Econ. J., vol. 99, no. 394, pp. 201–203, Mar. 1989.

[26] A. Abdul-Rahman and S. Hailes, “Supporting trust in virtual communities,” in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, 2000, p. 9 pp. vol.1–.

[27] S. Marti and H. Garcia-Molina, “Taxonomy of Trust: Categorizing P2P Reputation Systems,” Comput Netw, vol. 50, no. 4, pp. 472–484, Mar. 2006.

[28] F. Gomez Mármol and G. Martínez Pérez, “Towards Pre-standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems,” Comput Stand Interfaces, vol. 32, no. 4, pp. 185–196, Jun. 2010.

[29] A. Boukerch, L. Xu, and K. EL-Khatib, "Trust-based Security for Wireless Ad Hoc and Sensor Networks," Comput Commun, vol. 30, no. 11–12, pp. 2413–2427, Sep. 2007

Mohammed Aseeri, currently is a Researcher at Faculty of Information Sciences & Engineering, University of Canberra, Australia. Mohammed was working as a Head of the Maritimes Studies Section - Ministry of Interior - Border Guard, Saudi Arabia. He has a Bachelor's Degree in Electrical Engineering and Computer Engineering an MSc in Electrical Engineering and Computer Engineering, Electronics and Communications from the King Abdulaziz University and a PhD in Electronics from the University of Kent, Canterbury, England also he has an authorized certificate as consultant Engineer from SEC. His previous experiences include Project Manager, Electronic Surveillance Systems programs and projects of sensitive surveillance systems. Mohammed has also written and authored several papers on Field Programmable Gate Array (FPGA) as a new approach to implement the chaotic generators, on digital security as well as on Strategic and Secure Planning. Aseeri has published about twenty seven papers in high level of the IEEE and other Journals and International conference.

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 has obtained his PhD at the UC in 2014, 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.

Ahmed Al Ghamdi was works as a Head of the Organization Department of the operation department, Ministry of Interior, Border Guard, Saudi Arabia. He has a Bachelor's Degree in Military and MSc in IT and a PhD in IT from Lester University, England. His previous experiences include Project Manager, IT Surveillance Systems at the Interior Ministry Border Guards. Ahmed has also written and authored several papers on his Field. He has published many papers in high level of international conference.