A Novel Trust and Reputation Model Based WSN Technology to Secure Border Surveillance

Ahmed Al Ghamdi, Mohammed Aseeri, and Muhammad Raisuddin Ahmed

***Abstract*—Border surveillance systems have recently came into attention to address the concerns about national security. Conventional border surveillance or petrol systems consist of check points and border troops. The existing system for surveillance suffers from intensive human involvement. The recent technology is expensive as it requires using high-tech devices e.g. Unmanned aerial vehicles, unattended ground sensors, and surveillance towers equipped with Radar and camera sensors. These techniques suffer with problems such as high false alarm rate and for communication line of sight is necessary. In such surveillance system wireless sensor network is cost effective and efficient for event detection in the large area with multi hope communications. Using Wireless Sensor Network (WSN) the task of object tracking or event detection has been investigated but not much attention was given to secure the border. In this paper the security analysis of the border and a trust and reputation based WSN is presented secure border surveillance with some simulation results.**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. Introduction

Wireless sensor network (WSN) based system has become a popular application for border monitoring. Depending on the mission needs and scenario different kinds of wireless sensor nodes are embedded with the network, which gather verity of raw data that are than manage and refined to send to the monitoring base station. For example in order to detect and track trespassers or moving objects in border WSN nodes can be equipped with wide range of infrared sensors. A trespasser will try to manipulate the WSN node in a way for unattended crossing of the border with consideration of the WSN construction of the node. The sensor nodes consists a transceiver unit (combination of transmitter and receiver), a restricted memory processing unit, a sensing unit as well as a battery with limited power. Thus, for any application overhead of computation and communication is low.

To ensure the functionality of border security system with WSN, especially in malicious environments, security mechanisms become essential for all kinds of sensor networks. However, the resource constrains in the sensor nodes of a WSN and multichip communications in open wireless channel make the security of WSN even more heavy challenge. Since sensor nodes can (or have to) also be deployed in the hostile environment without any temper resistant protection. The nodes deployed in a network are relatively easy to be compromised, which is the case that the nodes are out of the system control and an adversary can easily get full access to those nodes

Nevertheless, this kind of networks has its own drawbacks. Their wireless way of communication, their battery and bandwidth constraints or their location in open environments, for example, lead them to some security threats. Recently, trust and reputation management has become a novel way of dealing with some of these important issues. Thus, several trust and/or reputation models over WSNs [1]-[4] have been developed and studied in this paper.

Moreover, one of the first issues to solve in order to achieve that expected improvement is to assure a minimum level of security in such a restrictive environment. Even more, ensuring confidence between every pair of interacting nodes is a critical issue in this kind of networks. Under these conditions we present in this paper a bio-inspired trust and reputation model, called BTRM-WSN, based on ant colony systems aiming at providing trust and reputation in WSNs. simulation results demonstrate the accuracy of our novel way.

The rest of the paper is organized as follows: Section II presents related works to secure the border. In Section III consists of the common attacker model in the border. Section IV we present our trust and reputation model. Section V describes the Result and Section VI is conclusion.

II. Related Works

Several works has been done in the past in the field of secure surveillance with WSN for the border, military and academic purpose. The early work done by Yang et al. [5], shown how to organize sensor nodes as a logical tree so as to facilitate in-network data processing and to reduce the total communication cost incurred by object tracking. Xu et al. [6] proposed the Dual Prediction Reporting (DPR) mechanism, in which the sensor nodes make intelligent decisions about whether or not to send updates of objects movement states to the base station and thus save energy. Yang et al. [7] proposed an architecture which is able to track targets with random movement patterns with accuracy over a wide range of target speed. Arora et al.[8] developed an experimental wireless sensor network for distributed intrusion detection but it is not autonomic.

These methods in the field of border object tracking and surveillance does not provide full security solutions as it fails

Manuscript received November 4, 2012; revised November 18, 2012.

Ahmed Al Ghamdi and Mohammed Aseeri are with the Border Guard, MOI, Saudi Arabia (e-mail: dr.ammg@gmail.com, aseeri50@hotmail.com)

Muhammad Raisuddin Ahmed is with University of Canberra, ISE, Australia (e-mail: muhammad.ahmed@canberra.edu.au)

in malicious environment.

III. Attacker Model in Border

In the malicious environment with compromised node it is possible to gain the knowledge of the WSN nodes internal memory and cryptographic information because compromised node act as a legitimate node in the network. So, the node accessibility allows the attacker to reprogram the node. The attacked or reprogramed node consider as compromised node or internal attacker.

Most important task of the border surveillance system is to detect the unusual event and report that to the base station securely with the location information. The unusual event normally represented by alarms which need to be sent to the base station instantly. Attacker main goal to perform the attack can be classified as create delay in the node, stop the alarm, massage manipulation and false alarm. The attacks are discussed as follows.

Create delay: the attacker will not take any attempt to prevent the report but the aim will be to incorporate the sufficient delay in the alarm. So, by the time the report reaches the base station the unusual event already occurred means the trespasser has already crossed the border. This could happen through collision attack occur.

Stop the alarm: this can occur when the compromised nodes deny forward, dropping or creating the appropriate massage. The attacker try the incorporate the congestion along the path and try to create a partition in the network to cut of the network connectivity with the node.

Massage manipulation: the attacker try to change the location or timing information before it sent out to the base station. Type of attack happen in the network is wormhole or reply 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 neighbors, when they are actually in different parts of the network.

False alarm: injection of massage by the attacker in Denial of Service (DoS) attack or record the massage than reply the same massage to the base station. So, it interesting false alarm massage can occur in the network uninformed.

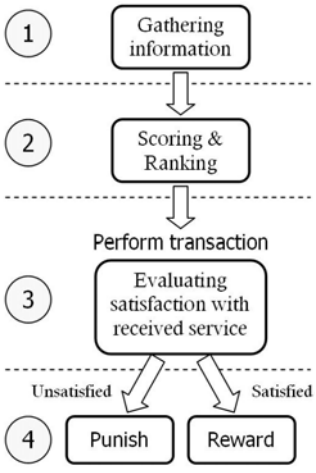

Fig. 1. Generic trust and reputation model [9]

IV. Trust and Reputation Model for WSN

Each trust and reputation model has its own specific characteristics and particularities. However, we share the same abstract schema or pattern about what steps have to be given in order to complete a whole transaction in a distributed system making use of a trust and/or reputation model.

Therefore, one of the main targets followed by our work was to design and provide a trust and reputation models interface as generic as possible for WSN. So initially, we identified the four main steps for our model following the paper [12], [13] which was done in TRMsim. Figure 1 shows these steps. We assume that the nodes are randomly distributed.

In our model present a trust and reputation model for WSNs, called BTRM-WSN (Bio-inspired Trust and Reputation Model for Wireless Sensor Networks)

BTRM-WSN is aimed to achieve to most trustworthy path leading to the most reputable node in a WSN offering a certain service. It is based on the bio-inspired algorithm of ant colony system (ACS) but, due to the specific restrictions and limitations found in WSNs, the ACS cannot be directly applied.

In our model, for instance, every node maintains a pheromone trace for each of its neighbors. This pheromone traces $\tau \in [0, 1]$ will determine the probability of ants choosing a certain route or another, and can be seen as the amount of trust given by a node to other one.

The heuristic values $\eta \in [0, 1]$, however, are defined as the inverse of the delay transmission time between two nodes (or the inverse of the distance between them). The fact that every node controls its own pheromone traces and heuristic values, and no one else but it can modify them can become an important security threat.

Algorithm 1 BTRM-WSN
1) while (condition) do
2) for k = 1 to Number_of_ants do
3) Sk ←initial sensor (client)
4) Launch ant k
5) do
6) for every returned ant k do
7) if (Q(Sk)>Q(Current_Best)) then
8) Current_Best←Sk
9) while (timeout does not expire) and
10) Num_returned_ants < %Number_of_ants
11) if (Q(Current_Best)>Q(Global_Best)) then
12) Global_Best←Current_Best
13) Pheromone_global_updating
14) (Global_Best,Q(Global_Best), ρ)
15) return Global_Best

V. Result

In our simulation model we have distributed the network by using TRMsim. To test the accuracy of every simulated trust and reputation model we have included two security threats following [15]. In Fig. 2 we can observe that a simulation over 10 random dynamic WSNs (with 100 sensors each one) has been carried out using BTRM-WSN model.

There were a 15% of clients, an 8.5% (85% · 10%) of relay sensors, a 53.55% (85% · 90%. 70%) of malicious servers and a 22.95% (85% · 90% · 30%) of benevolent ones. The average number of hops needed to reach the most trustworthy server was 6.04 and the average percentage of times that the model selected a benevolent server as the most trustworthy one was more than 90% and going almost 100% which shown in Fig. 4.

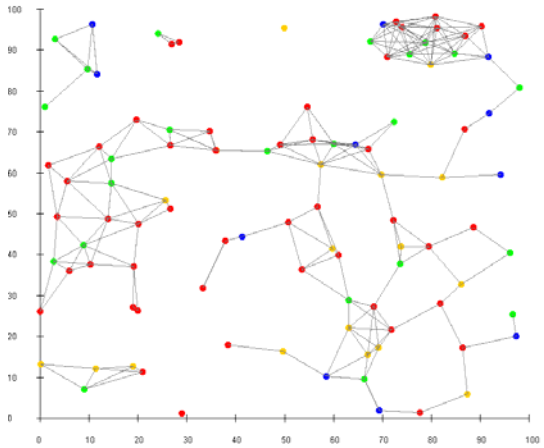

Fig. 2. The wireless sensor networks

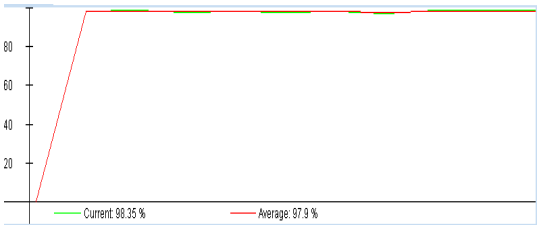

Fig. 3. The accuracy

VI. Conclusion

The Border surveillance system is a typical domain for the deployment of wireless sensor network. An analysis of possible attacks in the system and the trust and reputation model WSN to secure the border presented in this paper.

References

[1] F. G. M´armol and G. M. P´erez, "Providing Trust in WirelessSensor Networks using a Bio-inspired Technique," in *Proceedings of the Networking and Electronic Commerce Research Conference*, NAEC'08, 2008.

[2] A. Boukerche, L. Xu, and K. E. Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2413–2427, 2007.

[3] S. Buchegger and J. Y. L. Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," in *Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems*, Cambridge MA, USA, 2004.

[4] F. Almen´arez, A. Mar´ın, C. Campo, and C. Garc´ıa, *A pervasive trust management model for dynamic open environments*, in Privacy and Trust, Boston, USA: First Workshop on Pervasive Security and Trust, 2004.

[5] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulbarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita, "A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification and Tracking," in *Computer Networks*, vol. 46, no. 5, pp. 605–634, 2004.

[6] M. R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor Network," *International conference on information systems*, Kuala Lumpur, Malaysia, 2012.

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

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

[9] F. G. M´armol and G. M. P´erez, "TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks," *IEEE Communications Society publication in the IEEE ICC*, 2009

Ahmed AlGhamdi 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. Dr. Ahmed has also written and authored several papers on his Field. He has published many papers in high level of international conference.

Mohammed Alaseeri is currently is a Researcher at Faculty of Information Sciences & Engineering, University of Canberra, Australia. Dr Mohammed works 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 a authorized certificate as consultant Engineer from SEC. His previous experiences include Project Manager, Electronic Surveillance Systems, and Director of Draft Regulations for Electronic Surveillance Systems, SOS International GMDSS as well as supervision of several programs and projects of sensitive surveillance systems at the Interior Ministry Border Guards. Dr. Eng. 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. Dr Aseeri has published about twenty seven papers in high level of the IEEE and other Journals and international conference.

Muhammad Raisuddin Ahmed is currently serves as Lecturer 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, Engineers Australia in 2011. Besides, from March 2009 until 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.
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.