REVIEW OF SECURE TRUST AWARE ROUTING SCHEMES IN WSNs

Dilbag, Dr. Dinesh Kumar
Research Scholar
Guru Kashi University

Abstract: A wireless sensor network comprises a group of tiny, typically battery-powered devices and wireless infrastructure that monitor and record conditions in any number of environments. After from energy efficiency issues, security is another concern for such networks. These networks are unattended after deployment and can be easily compromised. Apart from various routing protocols that are developed to defend the network against various attacks, the trust models have also been proposed to detect the compromised nodes. This paper presents a review of routing techniques that uses trust model to protect the sensor networks against attacks. The trust model usually computes direct trust and indirect trust computation to check the node for the malicious activity.

Keywords: Wireless sensor network, Trust model, direct trust, indirect trust, energy efficiency.

I. INTRODUCTION

Nowadays, technology development in the fields of microelectromechanical system (MEMS) and wireless communication has facilitated the extensive distribution of WSNs. WSNs are composed of a large number of sensor nodes. In general, sensor nodes are reliable, accurate, flexible, inexpensive, and easy to deploy. Some areas and industries that are subject to environmental constraints rely on WSNs for data collection and monitoring [1]. They are widely used in many applications such as emergency response [2], healthcare monitoring [3], military, agriculture [4], environmental monitoring, and smart power grid [5]. The monitored results are sent to base station, where all the data are collected and sent to user through Internet. A large number of nodes are deployed in open and harsh environments to obtain data from sensor field. Hence, this large number of nodes collaborates with each other to monitor the area and send the monitored result to base station. As capability of the node is limited in terms of sensing area and communication range, there is no choice but cooperating with other nodes in the network. Hence, cooperation of the nodes is vital for the performance of WSNs. However, due to the characteristics of working environments (usually deployed in remote and unattended) and the way of wireless communication, WSNs are prone to sudden accidents failures and suffer from attacks of malicious nodes. Once a node is compromised, the availability and integrity of the network can be destroyed. In addition, it is difficult to predict the malicious attacks. Hence, network security is a vital issue, which needs to be addressed to guarantee correct operation of the whole network.

Recently, in the security field of wireless network, a great deal of research [6–8] has been carried out commonly using cryptography, authentication, and hash functions to improve the security of network. But in the security field of WSNs, the above traditional security mechanisms such as cryptography and authentication are not mostly suitable for processing capability constrained and energy limited WSNs due to the complexity and huge computing memory [9]. Furthermore, the traditional security mechanisms are widely and availably used to deal with external attacks but cannot solve insider or node misbehavior attacks effectively which are caused by the captured nodes [10]. In pursuit of the security of WSNs, trust and reputation mechanisms have proven to be more resilient against insider or node misbehavior attacks [10, 11].

This paper presents trust management among the nodes in sensor networks in next section. Section III presents the review of trust aware routing schemes for sensor networks. Finally the paper has been conclude in the last section.

II. TRUST MANAGEMENT

Recently, trust management is used in several applications including routing, data aggregation, access control, and intrusion detection. The term trust management (TM) is used jointly with the terms trust establishment and reputation system and discussed rarely. In the context of routing, TM deals with monitoring neighboring nodes during the transmissions, detecting misbehavior, estimating trust values based on detection results/recommendations, and propagation of trust value/recommendation.

The basic idea of trust based scheme is to quantify trust to describe the trustworthiness, reliability, or competence of individual nodes [5]. Trust management system can be implemented in various applications for security management such as secure protocol [8], secure data aggregation [12], trusted routing [13], and intrusion detection system [14]. Undoubtedly, the present achievements have greatly promoted related research in improving security of WSNs. Considerable research has been done on modeling and managing trust and reputation in WSNs. Many current studies have been done for trust establishment just only based on the communication interaction records between nodes without considering the data consistency, so they cannot be against attacks on data. While other studies combine multi-factors to calculate the trust value, the multi-trust sums up in weighted manner to compute the integrated trust. But the weights are obtained by expert opinion method or average weight method. The results of the prediction are subjective, which affect the scientific and flexibility of the trust decision. In many current trust models, the trust value is updated by a sliding time window using forgetting or aging mechanism. But the number of sliding windows is defined by expert opinion method. Once the number of the sliding time windows is confirmed, it is difficult to change. It makes the trust models unable to adapt to the dynamic changes of the network environment, which affects the accuracy of the result.

III. LITERATURE REVIEW

In this paper [15], a new Energy-aware and Secure Routing with Trust (ESRT) protocol is proposed for disaster relief operations of WSNs. Keeping resource-constrained characteristic of WSNs in mind, the design of ESRT is centered on trustworthiness and energy efficiency. In order to avoid the pre-mature energy depletion of trusted node, ESRT incorporates residual energy based threshold mechanism in route selection which helps to prolong the network lifetime. ESRT is capable of dynamically detecting and isolating misbehaving and faulty nodes during trust evaluation phase while energy awareness feature is incorporated in route setup phase of routing protocol which helps in better load balancing among trusted nodes. ESRT basically uses a composite routing metric which is calculated based on three factors: trust level, residual energy, number of hops. The net-effect of the composite routing function is to select the shortest route comprised of trusted and energy efficient nodes. The trust level of nodes is maintained by neighboring nodes using contemporary trust estimation mechanism. The trust estimation mechanism of ESRT involves direct trust, indirect trust and expected positive probability of nodes. Unlike most of the existing schemes, ESRT neither requires known geographic information nor tight time synchronization. More importantly, ESRT proves more resilient under heavy network load and demonstrates steady improvement in network performance. In addition, ESRT also sets up communication routes such that balanced energy consumption is achieved in reliable delivery of data packets. Using ESRT, only a set of nodes having sufficient energy and trust value are selected in active routing path. Moreover, ESRT makes use of shorter routes thereby reducing the number of transmissions and contention for the wireless medium. Simulation based evaluations of ESRT in NS-2 reveals better performance in terms of Throughput, average end-to-end delay, Normalized Routing Load (NRL) and Network lifetime as compared to other state-of-the-art.

In this paper [16], the authors presents an improved Weight-based Probabilistic Trust Evaluation (WPTE) scheme, based on beta probability distribution, for evaluating the trustworthiness of nodes. WPTE paves the way for trusted environment by isolating faulty and misbehaving nodes thereby providing reliable data delivery. The performance of WPTE scheme is evaluated and compared with state-of-art in terms of communication cost, trust convergence and degree of trustworthiness.

This paper [17] proposes a trust evaluation model and data fusion mechanism based on trust. First of all, it gives the model structure. Then, the calculation rules of trust are given. In the trust evaluation model, comprehensive trust consists of three parts: behavior trust, data trust, and historical trust. Data trust can be calculated by processing the sensor data. Based on the behavior of nodes in sensing and forwarding, the behavior trust is obtained. The initial value of historical trust is set to the maximum and updated with comprehensive trust. Comprehensive trust can be obtained by weighted calculation, and then the model is used to construct the trust list and guide the process of data fusion. Using the trust model, simulation results indicate that energy consumption can be reduced by an average of 15%. The detection rate of abnormal nodes is at least 10% higher than that of the lightweight and dependable trust system (LDTS) model. Therefore, this model has good performance in ensuring the reliability and credibility of the data. Moreover, the energy consumption of transmitting was greatly reduced.

In this paper [18], an efficient dynamic trust evaluation model (DTEM) for WSNs is proposed that aims to address the above problems. In the proposed trust model, the trust value is calculated considering multi-trust factors; it can achieve accurate trust evaluation. Moreover, DTEM can dynamically adjust the weights of direct trust and indirect trust. It reflects the dynamic adaptability of the trust computing. It also can dynamically adjust the parameters of the update mechanism to update the trust value to meet the actual needs of the network environment. The DTEM can be against various types of malicious attack and can be configured and effectively applied to different environments with different requirements.

In this work [19], a trust based Cluster Head selection mechanism using Firefly based metaheuristic is proposed to improve the security and network lifetime of the WSN. Firefly Algorithm (FA) is used as it handles combinational and numerical optimization multimodal problems efficiently. The proposed algorithm was evaluated using Mica testbed using 23 nodes and was also extensively simulated using MATLAB for large number of nodes to check the effectiveness of the proposed technique. Simulation results demonstrate the effectiveness of the proposed method for large number of nodes and the physical experimental setup shows performance improvement over LEACH.

The authors in [20] propose a trust mechanism, which evaluates communication trust and data trust for WSNs. Communication trust is computed from direct and indirect observations of the neighbor’s forwarding behavior. Direct trust is derived from the consistency of forwarding behavior. Indirect trust is derived from the neighbor’s observations translated into recommendations. They use weighted Dempster-Shaffer (D-S) theory to compute indirect trust. Data trust is computed by using median of sensor data. The authors’ present arguments and simulation results to show the effectiveness of the proposed algorithm against packet forwarding/modification attacks, bad mouthing attacks, collusion attacks, and on-off attacks. The proposed trust model helps data in WSNs to be more secure.

This paper [21] introduces the security and trust concepts in wireless sensor networks and explains the difference between them, stating that even though both terms are used interchangeably when defining a secure system, they are not the same. Highlighting that reputation partially affects trust. A survey of trust and reputation systems in various domains is conducted, with more details given to models in MTR and wireless sensor networks as they are closely related to each other and to our research interests. The methodologies used to model trust and their references are presented. The survey states that, even though researchers have started to explore the issue of trust in wireless sensor networks, they are still examining the trust associated with routing messages between nodes (binary events). However, wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete. This leads to the development of new trust models addressing the continuous data issue and also to combine the data trust and the communication trust to infer the total trust.

IV. CONCLUSION

The paper presents the review of trust aware routing schemes for sensor networks that are presented by various researchers. The nodes use the trust models compute the direct as well as indirect trust for the neighboring nodes. These trust computation are normally carried out considering the packet forwarding behavior of the nodes. One such technique consider energy efficiency as well. But it is the general trust model for packet dropping attacks. In future, the model can be modified for specific kind of attack.

References

1. R. D. Gomes, M. O. Adissi, T. A. da Silva, A. C. Filho, M. A. Spohn, and F. A. Belo, "Application of wireless sensor networks technology for induction motor monitoring in industrial environments," Intelligent Environmental Sensing, Volume 13 of Smart Sensors, Measurement and Instrumentation, pp. 227–277, Springer International Publishing, Cham, 2015.

2. M. M. Alam, D. Ben Arbia, and E. Ben Hamida, "Wearable wireless sensor networks for emergency response in public safety networks," Wireless Public Safety Networks, pp. 63–94, 2016.

3. M. Bhuiyan, G. Wang, J. Wu et al., "Dependable structural health monitoring using wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, pp. 1–47, 2015.

4. T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: the state-of-the-art in practice and future challenges," Computers and Electronics in Agriculture, Volume 118, pp. 66–84, 2015.

5. G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: a survey," Journal of Computer and System Sciences, Volume 80, no. 3, pp. 602–617, 2014.

6. H. Modares, A. Moravejosharieh, R. Salleh, and J. Lloret, "Security overview of wireless sensor network," Life Science Journal, Volume 10, no. 2, pp. 1627–1632, 2013.

7. R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks," Journal of Network and Computer Applications, Volume 34, no. 2, pp. 492–505, 2011.

8. R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "A secure protocol for spontaneous wireless Ad Hoc networks creation," IEEE Transactions on Parallel and Distributed Systems, Volume 24, no. 4, pp. 629–641, 2013.

9. J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," Electronic Notes in Theoretical Computer Science, Volume 197, no. 2, pp. 131–140, 2008.

10. M. Momani and S. Challa, "Survey of trust models in different network domains,"

International Journal of Ad hoc, Sensor & Ubiquitous Computing, Volume 1, no. 3, pp. 1–19, 2010.

11. A. Boukerch, L. Xu, and K. EL-Khatib, “Trust-based security for wireless ad hoc and sensor networks,” Computer Communications, Volume 30, no. 11-12, pp. 2413–2427, 2007.
12. Y. Liu, C.-X. Liu, and Q.-A. Zeng, “Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks,” Telecommunication Systems, Volume 62, no. 2, pp. 319–325, 2016.
13. X. Anita, M. A. Bhagyaveni, and J. M. L. Manickam, “Collaborative lightweight trust management scheme for wireless sensor networks,” Wireless Personal Communications, Volume 80, no. 1, pp. 117–140, 2015.
14. G. Rajeshkumar and K. R. Valluvan, “An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for Wireless Sensor Network,” Wireless Personal Communications, Volume. 94, no. 4, pp. 1993–2007, 2016.
15. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Abdul Waheed Khan, Khalid Haseeb, “Energy-aware and secure routing with trust for disaster response wireless sensor network”, Peer-to-Peer Networking and Applications, January 2017, Volume 10, Issue 1, pp 216–237.
16. Adnan Ahmed, Ali Raza Bhangwar, “WPTE: Weight-Based Probabilistic Trust Evaluation Scheme for WSN”, 5th International Conference on Future Internet of Things and Cloud Workshops, IEEE, November 2017.
17. Zhenguo Chen, Liqin Tian, Chuang Lin, “Trust Model of Wireless Sensor Networks and Its Application in Data Fusion”, Sensors (Basel), Volume 17(4), 2017 April, PMC5421663.
18. Zhengwang Ye, Tao Wen, Zhenyu Liu, Xiaoying Song, Chongguo Fu, “An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks”, Journal of Sensors
Volume 2017, Article ID 7864671, 16 pages.
19. S. Anbuchelian, S. Lokesh, Madhusudhanan Baskaran, “Improving security in Wireless Sensor Network using trust and metaheuristic algorithms”, 3rd International Conference on Computer and Information Sciences, IEEE, December 2016.
20. Vijender Busi Reddy, Sarma Venkataraman, Atul Negi, “Communication and Data Trust for Wireless Sensor Networks Using D–S Theory”, IEEE Sensors Journal, Volume: 17, Issue: 12, June15, 2017.
21. Sunny Kumar, Anuj Sharma, “Trust Based Shortest Path Routing Algorithm to Enhance

Security in WSN", IJCSMC, Vol. 6, Issue.
5, May 2017, pg.160 – 168.

JETIR