RESEARCH ARTICLE OPEN ACCESS

A Survey of provenance management in wireless sensor network

[1]Priyanka, [2]M.Devika
[1]M.Tech (VLSI Design) [2]Assistant Professor
Department Of ECE, Sathyabama University, Chennai, Tamilnadu, India.

Abstract
Wireless Sensor Networks have great potential for numerous applications such as military target tracking and surveillance, natural disaster relief, health monitoring and hazardous environment exploration and seismic sensing. This paper describes the concepts of efficient mechanism of provenance in WSNs as provenance respresents a key factor in evaluating the trustworthiness of sensor data. Data in sensor networks is processed by the multiple agents; data provenance plays an important role for assuring data trustworthiness. Due to energy and bandwidth limitations of WSNs, it is crucial that data provenance for these networks be as compress as possibles. To address such issues, this paper explained various proposed technique.
Key words: *provenance, sensor networks, trustworthiness.*

I. Introduction

Provenance helps gather, share and store the information which may lead to privacy and security concern in wireless sensor network. Security is one of the main characteristic of wireless sensor network affected with any attacks. Provenance, a mechanism of trust and reputation evaluation is an indispensable component to enchance the security of the entire network. Since provenance records the history of data acquisition and transmission, it is consideration as an effective mechanism to evaluate the trustworthiness and security of the data. It also provides the information about the operations performed on data.

Reducing the size of the provenance is crucial in WSN as it is composed of a large number of sensor nodes. The limitation of provenance in WSN is tight storage, limited energy and increased bandwidth consumption of the sensor node. Futhermore sensors often operate in an untrusted environment, where they may be subject to attacks. Provenace function is also deals with the detecting malicious node in network and to detect the packet drop in network.

Provenance trustworthiness is very important in large scale sensor network as it is deployed in a military information network and trust assessment is a crucial task. In the computational world, as all kinds of information can easily be changed, provenance becomes an important way of keeping track of alteration. Other applications of large scale network are medical monitoring, environmental monitoring, surveillance, home security, industrial machine monitoring etc.

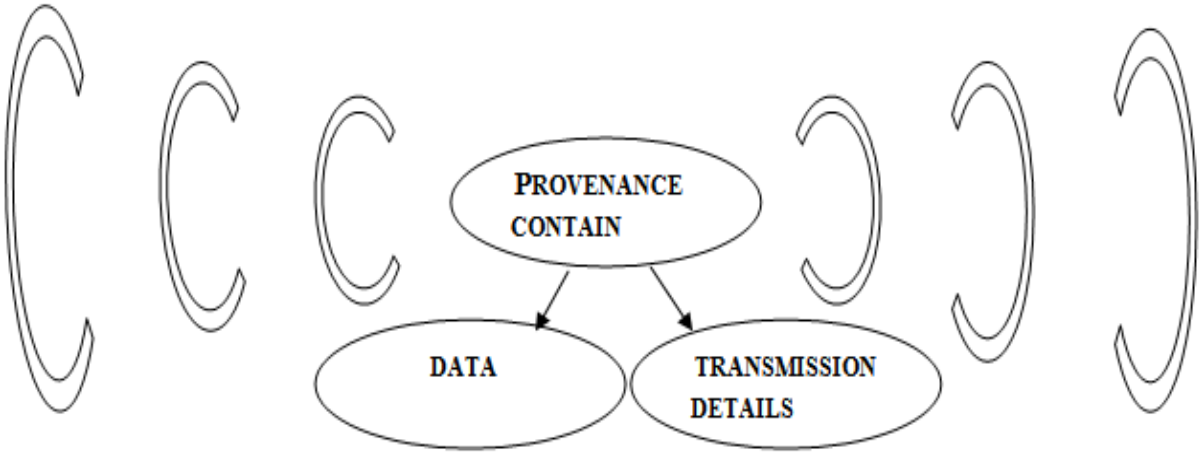

Fig (1): provenance model.

II. Different technique

Provenance management for sensor networks introduce several challenges such as low energy and bandwidth consumption, efficient storage and secure transmission.There are numerous techniques and method proposed for confidentiality, integrity, and trustworthy of secure provenance transmission in WSN.

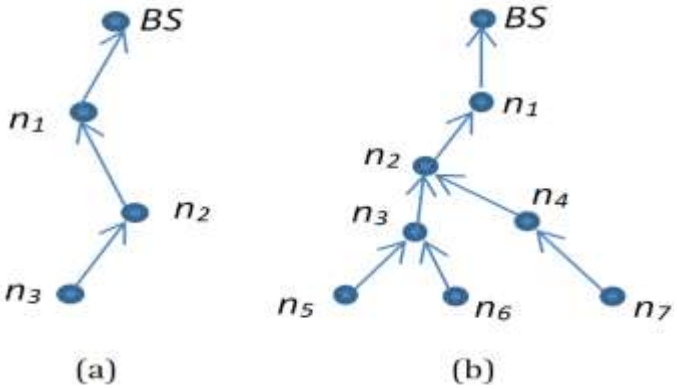

Fig (2): provenance graph.

2.1 Arithematic coding:

Compression scheme of provenance is vital in WSN to control over bandwith and energy consumption. Arithematic coding is one of the scheme which was proposed by the Syed Rafiul Hussian (2014) for secure data provenance compression. Arithematic coding ia a lossless data compression technique that assigns short codewords to more probable data symbols and longer codeword to less probable ones. Arithematic coding scheme uses floating point number to supports a limited numbers of bit to represents the digit after its decimal point.

2.2 Evaluation of Network Trust:

Trust is the challenging area in WSN as it is used in military operation. Gulustan dogan (2011) proposed a distributed intelligence in network. Which is faster than centralized approach and it is self adjusting information network, dataflow produce more accurate. Distributed system which evaluates the trust in the network that is more flexible and more responsive, which enchance the network trust in network. As trust is monitored and network is continuously restructured, our network remains trustworthy for a longer time.

2.3Dictionary based compression technique:

Chandela wang (2015) proposed a dictionary based provenance scheme which is lossless approach. In this method, each sensor node in the network stores a packet path dictionary. Which contain database of the provenance information as path indexes instead of the path itself in the provenance. This indexes are stored in a dictionary. With the support of this dictionary, a fixed size path index can be used to represent a path of arbitrary length. This technique gives secure provenance compression for wireless sensor network.

2.4ERUPT method:

ERUPT method main aim to reduce the energy consumption and to develop the trustworthy provenance in WSN, this method was proposed by S.M.Ifekharul alam (2014). This method determine a routing tree rooted at the base station with reduced number of active sensing nodes and select energy-efficient paths while ensuring that the selected paths contain trustworthy nodes and exhibit low correlation among them.

2.5Trustworthiness Evaluation in Multi-hop Networks

Xinlei wang (2010) proposed a evaluation which is done on the multi-hop network for provenance based information trustworthiness. This method considers two factors are path similarity and information similarity.This evaluation approach is unique by taking both information and path correlation for evaluation. Finally this method gives an information trust computation strategy based on information provenance.

2.6 A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks

Salmin sultana (2015) proposed light weighted and secure provenance in WSNs. For obtaining secure and lightweight provenance this method embedded the provenance information within a bloom filter that is transmitted along the data. On obtaining the packet the base station will check the information and it also check the packet drop attack. So here the single channel is used for data and provenance.

2.7Securing First-Hop Data Provenance for Bodyworn

Syed taha ali (2014) proposed a body worn device or secure data provenance transmission in WSNs. Here demonstrate the high correlation in channel measurment between the two endpoints. In this technique proposed wireless channel charactersistic between the sensor node and the basestation be used to generate link fingerprint. This process is secure since the fingerprint cannot be forged.

Fig(3): body worn device

III. Conclusion

This survey paper main approach is to show the different methodologies of secure compressed

provenance in WSNs. It also shows the various methods to save more energy and bandwidth. This paper goal is to improve the mechanism of provenance in wireless sensor networks by delievering the efficient transmission of secure provenance data along the transmitting medium, free from external threats.

References

[1]. S. I. Alam and S. Fahmy, "A practical approach for provenance transmission in wireless sensor networks," Ad Hoc Networks, vol. 16, no. 0, 2014.

[2]. H.-S. Lim, Y.-S. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, 2010.

[3]. Xinlei (Oscar) Wang, Kannan Govindan and Prasant Mohapatra,"Provenance-based Information Trustworthiness Evaluation in Multi-hop Networks," IEEE globecom-2010.

[4]. I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, 2002.

[5]. K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., 2006.

[6]. Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, 2005.

[7]. R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

[8]. Syed Rafiul Hussain, Changda Wang, Salmin Sultana, and Elisa Bertino, "Secure Data Provenance Compression Using Arithmetic Coding in Wireless Sensor Networks", 2014.

[9]. B. Shebaro, S. Sultana, S. R. Gopavaram, and E. Bertino, "Demonstrating a lightweight data provenance for sensor networks," in ACM Conference on Computer and Communications Security, 2012.

[10]. S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure provenance scheme for wireless sensor networks," in 2012 IEEE 18th International Conference on Parallel and Distributed Systems.

[11]. S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 99, 2014.

[12]. Gulustan Dogan, Theodore Brown, Kannan Govindan, Mohammad Maifi Hasan Khan, Tarek Abdelzaher, Prasant Mohapatra, Jin-Hee Cho, "Evaluation of Network Trust Using Provenance Based on Distributed Local Intelligence" in 2011 military communication conference track 4-middleware services and application.

[13]. D. Crawl and I. Altintas. A provenance-based fault tolerance mechanism for scientific workflows. Provenance and Annotation of Data and Processes, 2008.

[14]. S. Davidson and J. Freire. Provenance and scientific workflows: challenges and opportunities. In SIGMOD Conference, Citeseer, 2008.

[15]. J. Golbeck and A. Mannes. Using trust and provenance for content filtering on the semantic web. In Proceedings of the Models of Trust for the Web Workshop. Citeseer, 2006.

[16]. N. Heo and P. Varshney. An intelligent deployment and clustering algorithm for a distributed mobile sensor network. In Systems, Man and Cybernetics, 2003. IEEE International Conference on, volume 5, IEEE, 2003.

[17]. S. M. Iftekharul Alam, David K. Y. Yau, Sonia Fahmy, "ERUPT: Energy-efficient tRUstworthy Provenance Trees for Wireless Sensor Networks", IEEE, 2014.

[18]. A. Doboli and et al., "Cities of the future: Employing wireless sensor networks for efficient decision making in complex environments," SUNYSB, Tech. Rep., April 2008, cEAS Technical Report Nr 831.

[19]. L. Mo, Y. He, Y. Liu, J. Zhao, S.-J. Tang, X.-Y. Li, and G. Dai, "Canopy closure estimates with greenorbs: Sustainable sensing in the forest," in *Proc. of ACM Sensys*, 2009.

[20]. X. Liu, "Quality of optical channels in wireless SCADA for offshore wind farms," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, 2012.

[21]. S. Ganeriwal, "Trustworthy sensor networks," Ph.D. dissertation, University of California, Los Angeles, 2006.