International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

A Secured Dictionary Based Provenance Compression for Wireless Sensor Networks

Navaneeth Mola & Arpitha Kotte

[1]M.Tech Student, Department of CSE, Talla Padmavathi College of Engineering, Warangal District, Telangana, India.

[2]Assistant Professor, Department of CSE, Talla Padmavathi College of Engineering, Warangal District, Telangana, India

Abstract:

A measure that the network of sensors are being deployed more and more It is the Infrastructure of the decision making, stories such as the Surveillance Systems of the battlefield and SCADA (Control of Supervision and Acquisition of Data) Systems, for What the Beneficiaries of decisions that are aware of the reliability of the collected data. It is crucial. To address this problem, proposed a Systematic method to evaluate the reliability of data elements. Our approach uses the origin of Data, as well as their values in the Trusted Counting Scores, it is feasible of, Quantitative Reliability Measures to Obtain Trusted Scores, proposing a Cyclical Framework That Reflects Inter-Independence property:. The confidence score of the data affects the confidence score of the network nodes that created and manipulated the data, and vice versa. The trusted scores of the data elements are calculated from their similarity of value and similarity from the origin similarity value Goes ... from the Beginning of "The More similar Values for the same Event, the mayor is the confidence score". Similar parenting sources are based on the principle that "the most diverse data sources with similar values, the higher the trust ratings are higher."

Index Terms—Provenance, dictionary based compression, sensor network

1. Introduction:

In a dynamic network environment, a mechanism of trustAnd the reputation evaluation is an indispensable component for a improve the security of the entire network. In this network The environment, the information transmissions and the exchange are some of the activities essential for the quality of the information It is essential for end users, especially for those responsible for decision making. Analyzer of the reliability of the information received Different nodes or network entities, decision makers can do soevaluate the quality of the information received from them I make the right decisions. In a multipol network, information are genres of a source node, p. eg, a sensor Can makes to go through a series of other intermediate nodes before Arriving at your destination, that is, the end user.Much work has been done on data protection Manipulation, for example, digital signature techniques, to guarantee data Integrity when the information is directed through various nodes. However, they do not solve the information problem trust Unreliable information can be entered a cause of two different reasons: unintentional errors & intentional behavior [1] Involuntary errors are caused due to the poor functionality of the hardware (for example, broken or obstructed sensors), malpositioning of the node or depleted batteries. Bad intentional behavior is caused by malicious attackers, providing data falsifies a purpose through a compromised node. By evaluating the reliability of the information, we need for considering not only the reliability of the sender but also the information procedure. Defined the the confidence of the information elements and the nodes, as well as information comes from the following way.

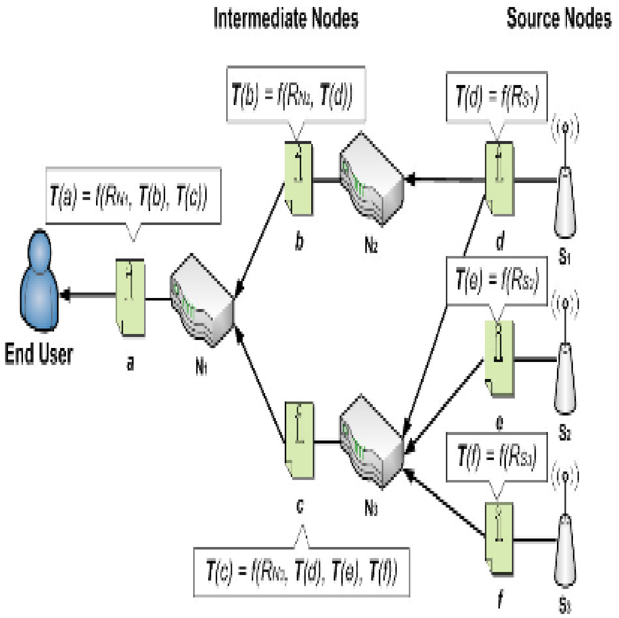


Fig. 1. An Example Network Scenario for Provenance based Information Trust Evaluation

2. Existing System

Existing Systems works on a probabilistic approach to encode the nodes' IDs into the provenance. And some of the other works use Bloom filter to encode the IDs of the nodes that are on a packet's path. These approaches minimize the size of provenance information by keeping only the nodes' IDs.Existing Works such as lightweight secure provenance scheme based on in-packet Bloom filter. This approach binds data and its provenance together and also chains the packet sequence numbers adjacently to detect provenance forgery and packet dropping attacks.

3. Disadvantages of Existing System:

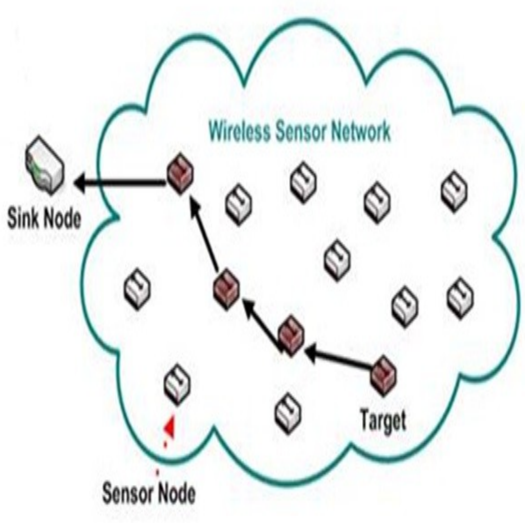
➢ The edges which refer the packet transmissions are discarded. Hence, those approaches are lossy provenance compression techniques.

➢ Only nodes' IDs are recorded in the data provenance.

➢ Unavoidable false positive in provenance decoding, and

➢ Increase in the provenance size with the number of nodes traversed in order to keep the false positive rate under a given threshold.

4. System Architecture



5. Proposed System:

➢ We propose a dictionary based provenance scheme which is the most compact and lossless scheme up to date.

➢ We design an efficient and distributed algorithm for encoding the provenance information as well as a centralized approach for its decoding.

➢ We introduce a secure packet sequence number generation mechanism and use the AM-FM sketch technique to secure the provenance.

➢ We perform a formal security analysis and an extensive performance evaluation of our proposed provenance scheme.

6. Advantages of Proposed System:

➢ We enclose path indexes instead of the path itself in the provenance.

➢ Hence, the size of the com-pressed provenance in our lossless approach is smaller than that of the existing lossy provenance schemes.

➢ By using the AM-FM sketch scheme and a secure packet sequence number generation technique, we ensure the security objectives of our scheme.

➢ During the process of provenance encoding, each node along a packet's path is assumed to be one of these three: data source node, forwarder node, and aggregator node.

➢ We design an efficient, and distributed algorithm for encoding the provenance information as well as a centralized approach for its decoding.

➢ We introduce a secure packet sequence number generation mechanism and use the AM-FM sketch technique to secure the provenance.

➢ We perform a formal security analysis and an extensive performance evaluation of our proposed provenance scheme.

7. Screen Shots

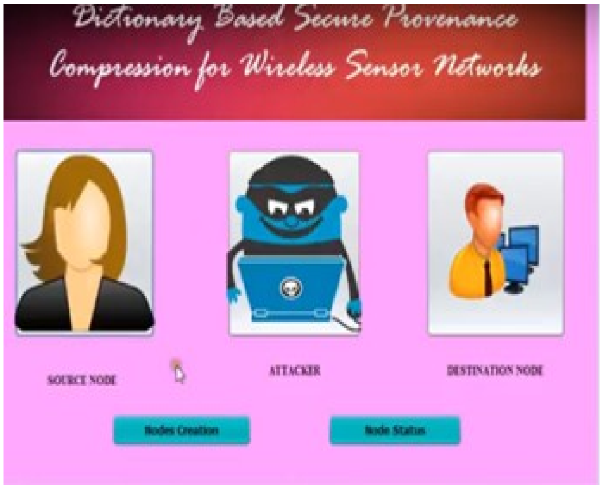

Dictionary Based Secure Provenance
Compression for Wireless Sensor Networks
SOURCE NODE
ATTACKER
DESTINATION NODE
Nodes Creation
Node Status

Fig 1: Home page

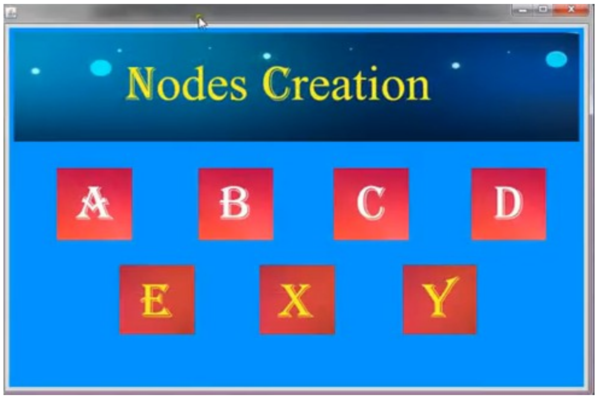


Fig 2: Nodes Creation

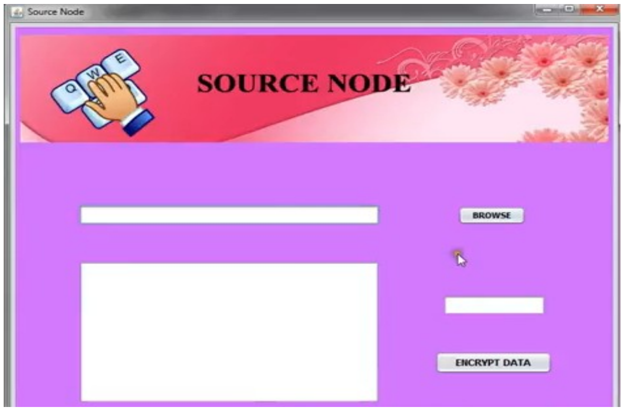
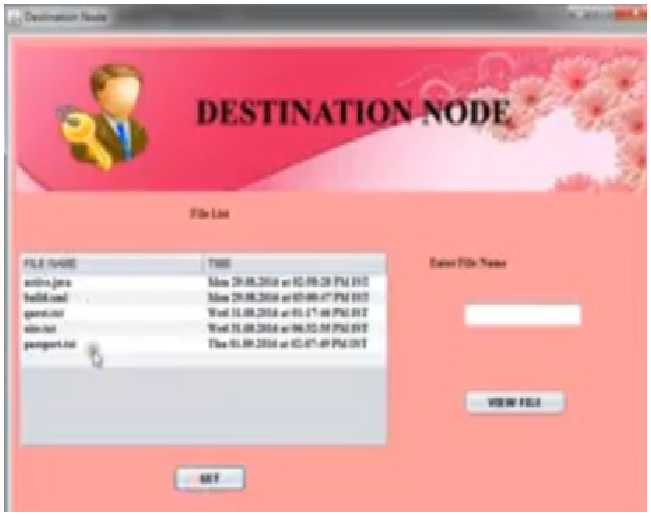


Fig 3: Source Node



FILE NAME	TIME
active.java	Mon 29.08.2016 at [illegible] PM IST
build.xml	Mon 29.08.2016 at [illegible] PM IST
guest.txt	Wed 31.08.2016 at [illegible] PM IST
site.txt	Wed 31.08.2016 at [illegible] PM IST
passport.txt	Thu 01.09.2016 at [illegible] PM IST

Fig 4: Destination Node

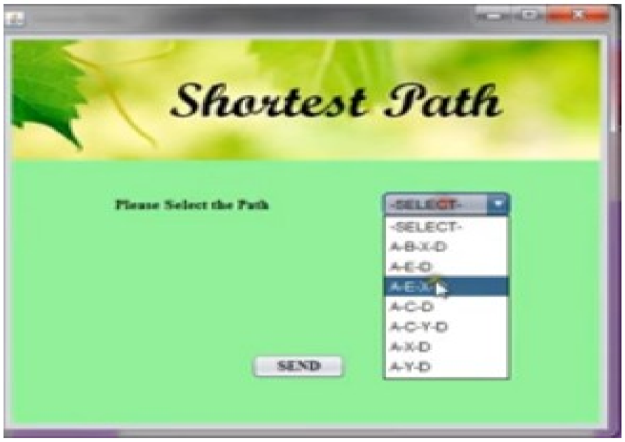


Fig 5: Shortest Path

7. Conclusion:

In this paper, we propose a dictionary based secure provenance scheme for wireless sensor networks. Using packet path dictionaries, we enclose path indexes instead of the path itself in the provenance. Hence, the size of the compressed provenance in our lossless approach is smaller than that of the existing lossy provenance schemes. By using the AM-FM sketch scheme and a secure packet sequence number generation technique, we ensure the security objectives of our scheme. Simulation and experimental results show that our scheme can save more energy and bandwidth than other existing provenance schemes.

REFERENCES

[1] H.-S. Lim, Y.-S.Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.

[2] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, “A lightweight secure provenance scheme for wireless sensor networks,” in Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst., 2012, pp. 101–108.

[3] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A virtual data system for representing, querying, and automating data derivation,” in Proc. 14th Int. Conf. Sci. Statist. Database Manage., 2002,m pp. 37–46.

[4] K.-K. Muniswamy-Reddy, D. A. Holland, U. Braun, and M. I. Seltzer, “Provenance-aware storage systems,” in Proc. USENIX Annu. Tech. Conf., General Track, 2006, pp. 43–56.

[5] S. M. I. Alam and S. Fahmy, “Energy-efficient provenance transmission in large-scale wireless sensor networks,” in Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw., 2011, pp. 1–6.

[6] B. Shebaro, S. Sultana, S. R. Gopavaram, and E. Bertino, “Demonstrating a lightweight data provenance for sensor networks,” in Proc.

ACM Conf. Comput. Commun. Security, 2012, pp. 1022–1024.

[7] A.-H. Jallad and T. Vladimirova, "Data-centricity in wireless sensor networks," in Guide to Wireless Sensor Networks (ser. Computer Communications and Networks). London, U.K.: Springer, 2009, pp. 183–204.

[8] D. Ma, "Secure feedback service in wireless sensor networks," in Information Security Practice and Experience. ser. Lecture Notes in Computer Science, vol. 4464, Springer, 2007, pp. 116–128.

[9] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in Proc. 31st Int. Conf. Distrib.Comput. Syst. Workshops, 2011, pp. 332–338.

[10] S. Ihara, Information Theory for Continuous Systems. Singapore: World Scientific, 1993.

[11] J. Ziv and A. Lempel, "A universal algorithm for sequential data compression," IEEE Trans. Inform. Theory, vol. 23, no. 3, pp. 337– 343, May 1977.

[12] J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," IEEE Trans. Inform. Theory, vol. 24, no. 5, pp. 530–536, Sep. 1978.

[13] M. Garofalakis, J. M. Hellerstein, P. Maniatis, and IEEE, "Proof sketches: Verifiable in-network aggregation," in Proc. IEEE 23rd Int. Conf. Data Eng., 2007, pp. 971–980.

[14] S. Madden, M. J. Franklin, J.M. Hellerstein, and W. Hong, "Tag: A tiny aggregation service for ad-hoc sensor networks," SIGOPS Oper. Syst. Rev., vol. 36, no. SI, pp. 131–146, Dec. 2002.

[15] P. Levis, N. Lee, M. Welsh, and D. Culler, "Tossim: Accurate and scalable simulation of entire tinyos applications," in Proc. 1st Int. Conf. Embedded Netw. Sens. Syst., 2003, pp. 126–137.

[16] 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 Trans. Dependable Secure Comput., vol. PP, no. 99, p. 1, 2013.

[17] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in Proc. 7th Conf. File Storage Technol., 2009, pp. 1–14.

[18] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. Int. Conf. Inform. Process. Sens. Netw, Apr. 2008, pp. 245–256.

[19] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in Proc. 2nd Int. Conf. Embedded Netw. Sens. Syst., 2004, pp. 162–175.

[20] W. Zhou, M. Sherr, T. Tao, X. Li, B. T. Loo, and Y. Mao, "Efficient querying and maintenance of network provenance at internetscale," in Proc. ACM SIGMOD Int. Conf. Manag. Data, 2010, pp. 615–626.

[21] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. T. Loo, and M. Sherr, "Secure network provenance," in Proc. 23rd ACM Symp. Oper. Syst. Principles, 2011, pp. 295–310.

[22] S. Chen and J. H. Reif, "Efficient lossless compression of trees and graphs," in Proc. IEEE Data Compression Conf. (DCC'96), Mar. 1996, p. 428.