Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2018 13 (3): 902-910

Secured Routing in Wireless Sensor Networks: To Avoid False Data Injection

Dr.C. Nalini

Received: 12 Jan 2018 ▪ Revised: 17 March 2018 ▪ Accepted: 10 April 2018

Abstract: In today's developing world a large amount of sensor networks are used in various real-time applications. Large amount of Data are streamed from multiple sources through intermediate processing nodes that share information throughout the network. Some of the domains where these Sensor networks are used include cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data goes through various nodes to complete a path from producer system to consumer system. Malicious attacks are possible in between. This project hereby introduces an in-packet bloom filter, which will keep the track of provenance details of each packet separately. This proposal is about a novel lightweight scheme to securely transmit provenance for sensor data. It introduces efficient mechanisms for provenance verification and reconstruction at the base station through decoding of the provenance details. This extends the secure provenance scheme with functionality to detect packet drop attacks. The goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs.

Keywords: Provenance Encoding, Primary Key, Inbloom Filters.

INTRODUCTION

Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station (BS) that performs decision-making. In a multi-hop sensor network, data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. It is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs.

PROBLEM IDENTIFICATION

The provenance modeling, collection, and querying has been studied extensively for workflows and curate databases; provenance in sensor networks has not been properly addressed. It does not consider denial of service attacks such as the complete removal of provenance, since a data packet with no provenance records will make the data highly suspicious and hence generate an alarm at the Base S. Any confidentiality cannot gain any knowledge about data provenance by analyzing the contents of a packet. Integrity, acting alone or colluding with others, cannot add or remove non-colluding nodes from the provenance of benign data (i.e., data generated by benign nodes) without being detected. Freshness, cannot replay captured data and provenance without being detected by the Base Station.

It is also important to provide Data-Provenance Binding, i.e., a coupling between data and provenance so that an attacker cannot successfully drop or alter the legitimate data while retaining the provenance, or swap the provenance of two packets. In a distributed aggregate computation to verify that the final result has not been perturbed by more than a small error bound with high probability. It do not address the issue of recovery once a malicious node is detected. If there is an intermediate packet drop, some nodes on the path do not receive the packet. When one-way hash functions are used to insert elements in the BF, the identities of the inserted elements cannot be reconstructed from the BF representation.

Dr.C. Nalini, Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: nalini.cse@bharathuniv.ac.in

RELATED WORKS

[1] *H. Lim, Y. Moon, and E. Bertino,* ***"Provenance-Based Trustworthiness Assessment in Sensor Networks,"*** As sensor networks are being increasingly deployed in decision-making infrastructures such as battle field monitoring systems and SCADA (Supervisory Control and Data Acquisition) systems, making decision makers aware of the trustworthiness of the collected data is a crucial.
*T*his *approach uses the data provenance as well as their values in computing trust scores, that is, quantitative measures of trust worthiness. The provenance similarity is based on the principle that "the more different data provenances with similar values, the higher the trust scores".*

[2] *Foster, J. Vockler, M. Wilde, and Y. Zhao,* ***"Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation,"*** A lot of scientific data is not obtained from measurements but rather derived from other data by the application of computational procedures. We hypothesize that explicit representation of these procedures can enable documentation of data provenance, discovery of available methods, and on-demand data generation (so-called "virtual data").

[3] A Chimera virtual data system, which combines a virtual data catalog for representing data derivation procedures and derived data, with a virtual data language interpreter that translates user requests into data definition and query operations on the database.

[4] *K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer,* ***"Provenance-Aware Storage systems,"*** A Provenance-Aware Storage System (PASS) is a storage system that automatically collects and maintains provenance or lineage, the complete history or ancestry of an item. We discuss the advantages of treating provenance as meta-data collected and maintained by the storage system, rather than as manual annotations stored in a separately administered database. We describe a PASS implementation, discussing the challenges it presents, performance cost it incurs, and the new functionality it enables. We show that with reasonable overhead, we can provide useful functionality not available in today's file systems or provenance management systems.

[5] *Y. Simmhan, B. Plale, and D. Gannon,* ***"A Survey of Data Provenance in E-Science,"*** Data management is growing in complexity as large scale applications take advantage of the loosely coupled resources brought together by grid middleware and by abundant storage capacity.
Metadata describing the data products used in and generated by these applications is essential to disambiguate the data and enable reuse. Data provenance, one kind of metadata, pertains to the derivation history of a data product starting from its original sources.

EXISTING SYSTEM

There are two main parts of the existing system.

- Pedigree captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet.
- ExSPAN describes the history and derivations of network state that result from the execution of a distributed protocol.

Few Points to Overcome

- This system does not address security concerns and is specific to some network use cases. This becomes a disadvantage.
- This system traces the source of a stream long after the process has completed. It reflects the importance of issues we addressed, it is not intended as a security mechanism, hence, does not deal with malicious attacks.

PROPOSED SYSTEM

1. The proposed technique relies on in-packet Bloom filters to encode provenance.
2. Here gets introduced an efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes.
3. It propose an in-packet Bloom filter (iBF) provenance-encoding scheme. The design efficient techniques for provenance decoding and verification at the base station. The detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.
4. A multihop wireless sensor network, co/nsisting of a number of sensor nodes and a base station that collects data from the network

5. Each data packet contains 1) a unique packet sequence number, 2) a data value, and 3) provenance.

The sequence number is attached to the packet by the data source, and all nodes use the same sequence number for a given round. The sequence number integrity is ensured through MACs.

OVERALL ARCHITECTURE

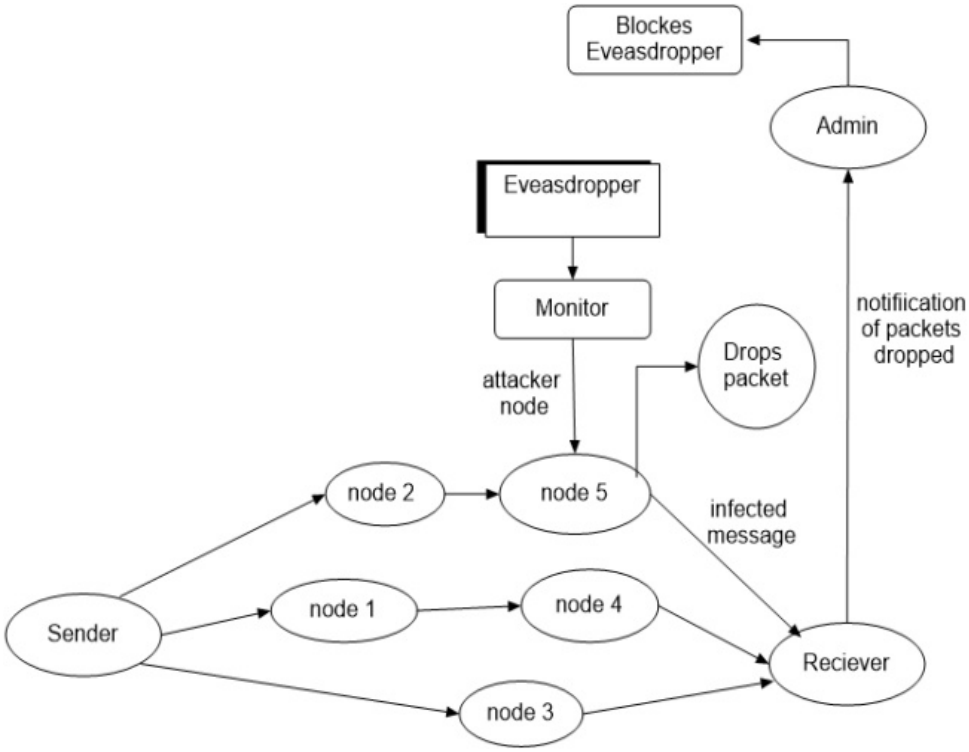

Figure 1: Wireless sensor network showing the malicious attacker in between the regular nodes

MODULES

1. Provenance Verification

In verification of the modules it processes the Key generation, decryption, and also the key exchanging, sent to receiver module. The RSA used here involves a public key and a private Key**.** The public key can be known to everyone and is used for encrypting the messages. Messages encrypted with the public key can only be decrypted using the private key which will act as the enhancing point of this paper. The keys for the RSA algorithm are generated. In Provenance Collection, receiver module receives a packet data suspicious means place in suspicious box suppose, the data means placed in province box. The Base Station conducts the verification process not just only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance data of all the data packets involved.

2. Data Provenancce

Data provenance represents a key factor in evaluating the trustworthiness of sensor data.

Setup: the data producer sets up its signing key k and data consumer sets up its verification key k0 in a secure fashion that prevents malware from accessing the secret keys.

Sign (D, k): the data producer signs its data D with a secret key k, and outputs D along with its proof sig.

Verify (sig, D, k0): the data consumer uses key k0 to verify the signature sig of received data D to ensure its origin, and rejects the data if the verification fails.

3. Provnenance Encoding and Decoding

In provenance encoding strategy whereby each node on the path of a data packet actually securely embeds the provenance information within a Bloom filter (BF) which will then be transmitted along with the data. As soon as we receive the packet, the Base Station extracts and verifies the provenance information provided. This paper also devises an extension of the provenance encoding scheme that allows the Base Station to detect if a packet drop attack was done by aay malicious node through the transmission path. For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF.

4. ALGORITHM USED

1. Routing Algorithm

Routing is the process of selecting best paths in a network. In the past, the term routing also meant forwarding network traffic among networks. However, that latter function is better described as forwarding. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

This algorithm helps to find the connectivity between the Source and Destination. It checks for all nodes which are connected in network and retrieves to user. So, the user can know about the destination connectivity. In case there is no connectivity between the source and destination, it pops-up to the User. If connection is available, then the source can send the packets to destination through the corresponding path.

Some Common Thoughts

- The people in the digital world think that the data insecurity occurs only through hacking them.
- This is a great misconception.
- In fact, the biggest threat is that even when there is a tight security in the routing process by encoding and decoding, the data gets corrupted.
- This is because the data packets may go through various nodes when the attacker actually corrupts the original data by inserting malicious packets.

Key Generation Algorithm

Key generation algorithm is one of the algorithm used to generate an unique key to encrypt and decrypt the data. The same key has to be used both the sides to establish a relevant connection.

Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). Symmetric-key algorithms usually use a single shared key; which actually keeps the data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data.

Since public-key algorithms tend to be much slower than symmetric-key algorithms, modern systems such as TLS and SSH use a combination of the two: one party receives the other's public key, and encrypts a small piece of data (either a symmetric key or some data used to generate it). The remainder of the conversation uses a (typically faster) symmetric-key algorithm for encryption.

EXPERIMENTAL SETUP AND RESULT

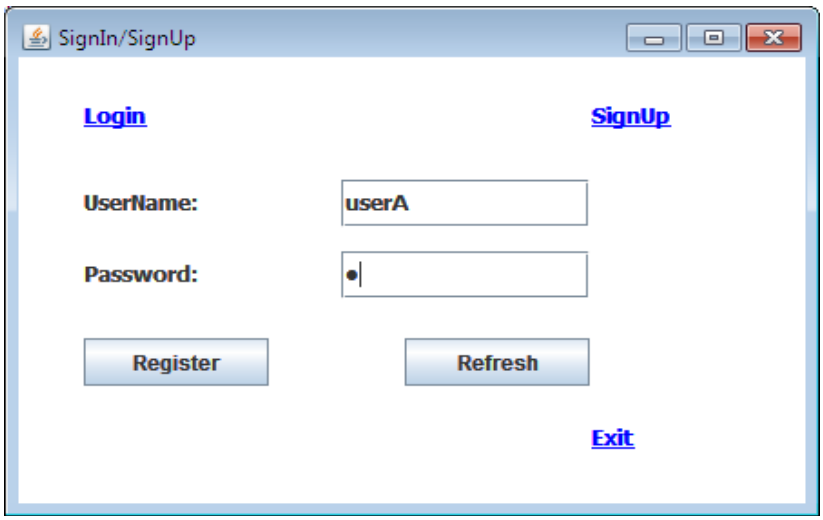

Fig. 2: Register and Login form

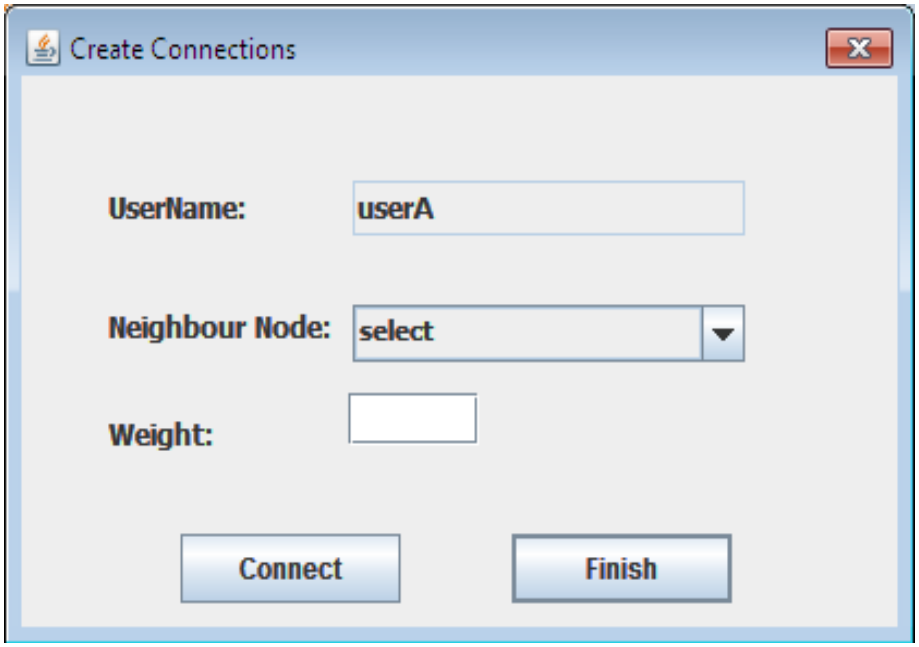

Fig. 3: Form to connect the nodes to create various paths.

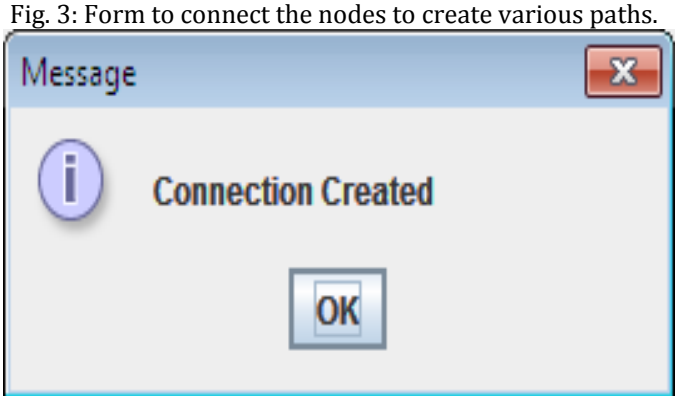

Fig. 4: Dialog box for showing the connection is established.

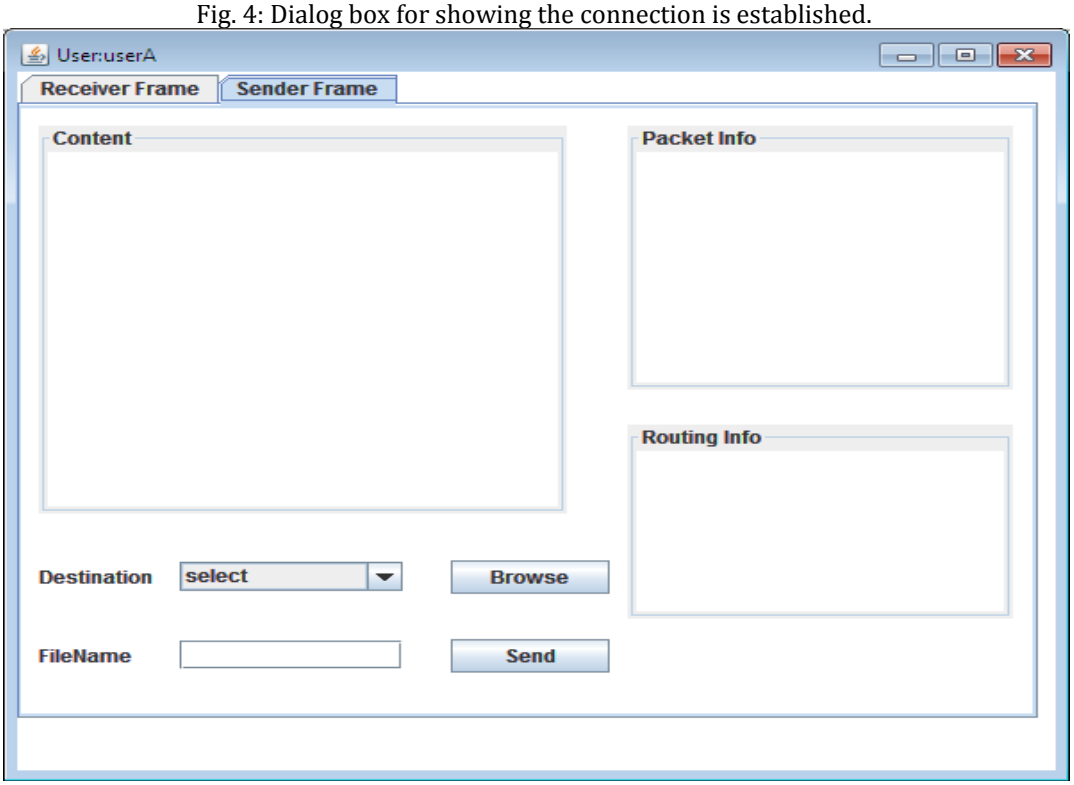

Fig. 5: User wise Sender and Receiver module to send or receive data

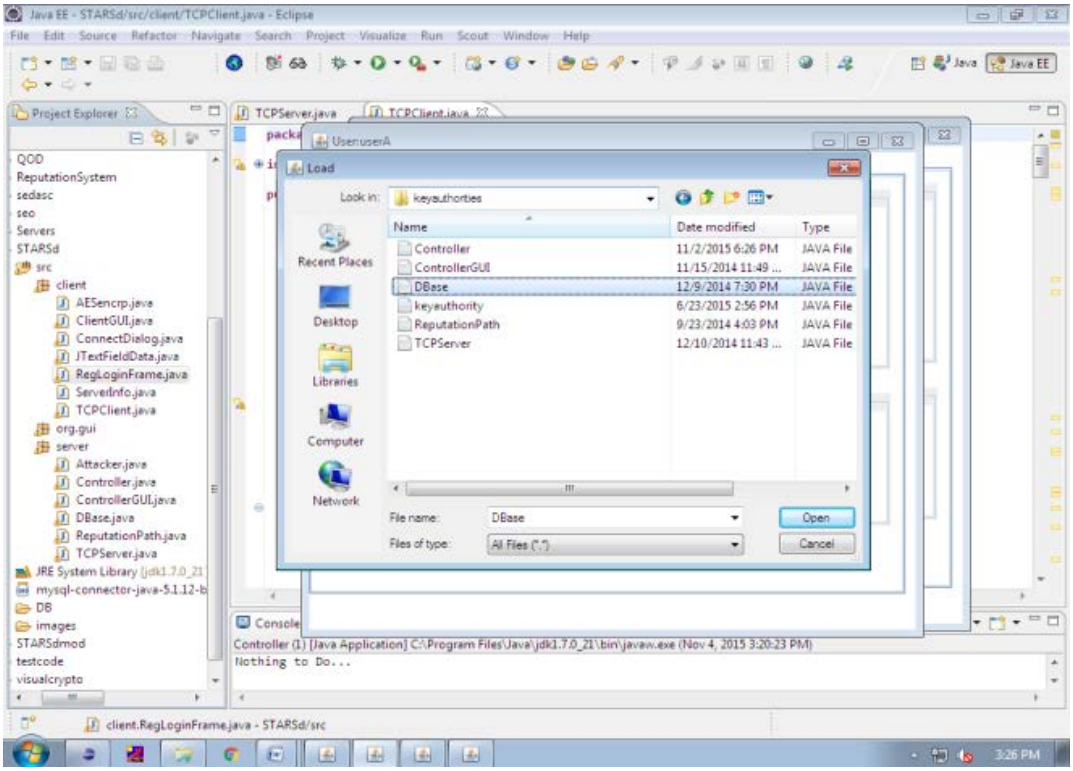

Fig. 6: Select text file from the computer

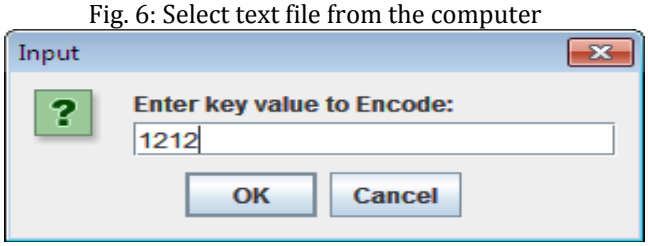

Fig. 7: Dialog box to encoding theory

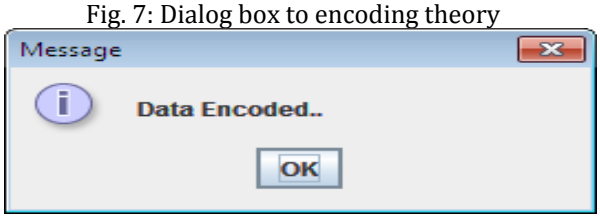

Fig. 8: Dialog box to show that the data has been encoded

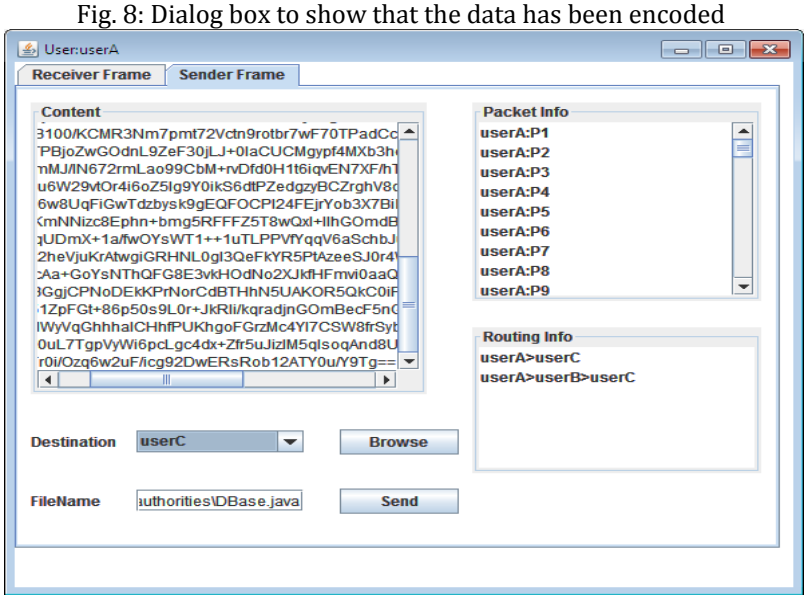

Fig. 9: Receiver modules receive the data

CONCLUSION

This paper addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The proposed system ensures confidentiality, integrity and freshness of provenance. Furthermore, the paper extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Till now we have come across the algorithms going to be used in the prevention of packet drops. Hence the data provenance will be used to detect packet drops and overcome it to enhance security.

REFERENCES

[1] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique. *Indian Journal of Science and Technology*, *6*(6), 4767-4771.

[2] Udayakumar, R., Kumaravel, A., & Rangarajan, K. (2013). Introducing an efficient programming paradigm for object-oriented distributed systems. *Indian Journal of Science and Technology*, *6*(5S), 4596-4603.

[3] Mageswaran, S.U., & Sekhar, N.G. (2013). Reactive power contribution of multiple STATCOM using particle swarm optimization. *International Journal of Engineering & Technology*, *5*(1), 122-126.

[4] Giri, R.K., & Saikia, M. (2013). Multipath routing for admission control and load balancing in wireless mesh networks. *International Review on Computers and Software*, *8*(3), 779-785.

[5] Padmapriya, G., Manikandan, A., Krishnasamy, V., Jaganathan, S.K., & Antony, S.A. (2016). Spinel NixZn1− xFe2O4 (0.0≤ x≤ 1.0) nano-photocatalysts: synthesis, characterization and photocatalytic degradation of methylene blue dye. *Journal of Molecular Structure*, *1119*, 39-47.

[6] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., & Sundar Raj, M. (2013). Analysis of chaotic DC-DC converter using wavelet transform. *Middle-East Journal of Scientific Research*, *16*(12), 1813-1819.

[7] Lokesh, K., Kavitha, G., Manikandan, E., Mani, G.K., Kaviyarasu, K., Rayappan, J.B.B., ... & Maaza, M. (2016). Effective ammonia detection using n-ZnO/p-NiO heterostructured nanofibers. *IEEE Sensors Journal*, *16*(8), 2477-2483.

[8] Abraham, A.G., Manikandan, A., Manikandan, E., Vadivel, S., Jaganathan, S.K., Baykal, A., & Renganathan, P.S. (2018). Enhanced magneto-optical and photo-catalytic properties of transition metal cobalt (Co2+ ions) doped spinel MgFe2O4 ferrite nanocomposites. *Journal of Magnetism and Magnetic Materials*, *452*, 380-388.

[9] Kennedy, J., Fang, F., Futter, J., Leveneur, J., Murmu, P.P., Panin, G.N., & Manikandan, E. (2017). Synthesis and enhanced field emission of zinc oxide incorporated carbon nanotubes. *Diamond and Related Materials*, *71*, 79-84.

[10] Teresita, V.M., Manikandan, A., Josephine, B.A., Sujatha, S., & Antony, S.A. (2016). Electromagnetic properties and humidity-sensing studies of magnetically recoverable LaMg x Fe 1− x O 3− δ perovskites nano-photocatalysts by sol-gel route. *Journal of Superconductivity and Novel Magnetism*, *29*(6), 1691-1701.

[11] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of pure and doped bis thiourea zinc acetate: Semiorganic nonlinear optical single crystals. *Current applied physics*, *9*(5), 1054-1061.

[12] Jayalakshmi, V., & Gunasekar, N.O. (2013). Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag/swell. *International Conference on Energy Efficient Technologies for Sustainability*, 1036-1040.

[13] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Optical ring architecture performance evaluation using ordinary receiver. *Indian Journal of Science and Technology*, *6*(6), 4742-4747.

[14] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Performance analysis of resilient ftth architecture with protection mechanism. *Indian Journal of Science and Technology*, *6*(6), 4737-4741.

[15] Saravanan, T., Srinivasan, V., & Sandiya, V.P. (2013). A two stage DC-DC converter with isolation for renewable energy applications. *Indian Journal of Science and Technology*, *6*(6), 4824-4830.

[16] Sundarraj, M. (2013). Study of compact ventilator. *Middle-East Journal of Scientific Research*, *16*(12), 1741-1743.

[17] Thema, F.T., Manikandan, E., Gurib-Fakim, A., & Maaza, M. (2016). Single phase Bunsenite NiO nanoparticles green synthesis by Agathosma betulina natural extract. *Journal of alloys and compounds*, *657*, 655-661.

[18] Sathyaseelan, B., Manikandan, E., Sivakumar, K., Kennedy, J., & Maaza, M. (2015). Enhanced visible photoluminescent and structural properties of ZnO/KIT-6 nanoporous materials for white light emitting diode (w-LED) application. *Journal of Alloys and Compounds*, *651*, 479-482.

[19] Gopalakrishnan, K., Prem Jeya Kumar, M., Sundeep Aanand, J., & Udayakumar, R. (2013). Analysis of static and dynamic load on hydrostatic bearing with variable viscosity and pressure. *Indian Journal of Science and Technology,* 6(6), 4783-4788.

[20] Prabhu, M.R., Reji, V., & Sivabalan, A. (2012). Improved radiation and bandwidth of triangular and star patch antenna. *Research Journal of Applied Sciences, Engineering and Technology*, *4*(12), 1740-1747.

[21] Arumugam, S. and Ramareddy, S. (2012). Simulation comparison of class D/ Class E inverter fed induction heating. *Journal of Electrical Engineering*, 12(2), 71-76.

[22] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). High data rate for coherent optical wired communication using DSP. *Indian Journal of Science and Technology*, *6*(6), 4772-4776.

[23] Nagarajan, C., & Madheswaran, M. (2012). Experimental Study and Steady State Stability Analysis of CLL-T Series Parallel Resonant Converter with Fuzzy Controller using State Space Analysis. *Iranian Journal of Electrical and Electronic Engineering*, *8*(3): 259-267.

[24] Gopalakrishnan, K., PremJeya Kumar, M., SundeepAanand, J., & Udayakumar, R. (2013). Thermal properties of doped azopolyester and its application. *Indian Journal of Science and Technology*, *6*(6), 4722-4725.

[25] Kumaravel A., Meetei O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *Indian Journal of Science and Technology*, *6*(5): 4560-4566.

[26] Kumaravel, A., & Pradeepa, R. (2013). Layered approach for predicting protein subcellular localization in yeast microarray data. *Indian Journal of Science and Technology*, *6*(5S), 4567-4571.

[27] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2016). Synthesis and analytical applications of photoluminescent carbon nanosheet by exfoliation of graphite oxide without purification. *Journal of Materials Science: Materials in Electronics*, *27*(12), 13080-13085.

[28] Mathubala, G., Manikandan, A., Antony, S.A., & Ramar, P. (2016). Photocatalytic degradation of methylene blue dye and magneto-optical studies of magnetically recyclable spinel NixMn1-xFe2O4 (x= 0.0–1.0) nanoparticles. *Journal of Molecular Structure*, *1113*, 79-87.

[29] Manikandan, E., Kennedy, J., Kavitha, G., Kaviyarasu, K., Maaza, M., Panigrahi, B.K., & Mudali, U.K. (2015). Hybrid nanostructured thin-films by PLD for enhanced field emission performance for radiation micro-nano dosimetry applications. *Journal of Alloys and Compounds*, *647*, 141-145.

[30] Kumaravel, A., & Meetei, O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *IEEE Conference on Information & Communication Technologies*: 1200-1205.

[31] Langeswaran, K., Gowthamkumar, S., Vijayaprakash, S., Revathy, R., & Balasubramanian, M.P. (2013). Influence of limonin on Wnt signalling molecule in HepG2 cell lines. *Journal of natural science, biology, and medicine*, *4*(1), 126-133.

[32] Srinivasan, V., & Saravanan, T. (2013). Analysis of harmonic at educational division using CA 8332. *Middle-East Journal of Scientific Research*, *16*(12), 1768-73.

[33] Josephine, B.A., Manikandan, A., Teresita, V.M., & Antony, S A. (2016). Fundamental study of LaMg x Cr 1− x O 3− δ perovskites nano-photocatalysts: sol-gel synthesis, characterization and humidity sensing. *Korean Journal of Chemical Engineering*, *33*(5), 1590-1598.

[34] Saravanan, T., Saritha, G., & Udayakumar, R. (2013). Robust H-Infinity Two Degree of Freedom Control for Electro Magnetic Suspension System. *Middle-East Journal of Scientific Research*, *18*(12), 1827-1831.

[35] Rajasulochana, P., Dhamotharan, R., Murugakoothan, P., Murugesan, S., & Krishnamoorthy, P. (2010). Biosynthesis and characterization of gold nanoparticles using the alga Kappaphycus alvarezii. *International Journal of Nanoscience*, *9*(05), 511-516.

[36] Slimani, Y., Güngüneş, H., Nawaz, M., Manikandan, A., El Sayed, H. S., Almessiere, M. A., & Baykal, A. (2018). Magneto-optical and microstructural properties of spinel cubic copper ferrites with Li-Al co-substitution. *Ceramics International*, *44*(12), 14242-14250.

[37] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., & Maaza, M. (2016). Rice husks as a sustainable source of high quality nanostructured silica for high performance Li-ion battery requital by sol-gel method–a review. *Adv. Mater. Lett*, *7*(9), 684-696.

[38] Ilayaraja, K., & Ambica, A. (2015). Spatial distribution of groundwater quality between injambakkamthiruvanmyiur areas, south east coast of India. *Nature Environment and Pollution Technology*, *14*(4), 771-776, 2015.

[39] Sharmila, S., Rebecca, L. J., Das, M.P., & Saduzzaman, M. (2012). Isolation and partial purification of protease from plant leaves. *Journal of Chemical and Pharmaceutical Research*, *4*(8), 3808-3812.

[40] Rajakumari, S.B., & Nalini, C. (2014). An efficient cost model for data storage with horizontal layout in the cloud. *Indian Journal of Science and Technology*, *7*(3), 45-46.

[41] Hemalatha, S., and Muthaiah, U. (2015). Security with Authorized Deduplication Compression Using JHF and DR Techniques in Hybrid Cloud. *Excel International Journal of Technology, Engineering and Management, 2*(1), 6-9.

[42] Shanmugapriya, P., and Kavitha, C. (2015). Remote Data Integrity Verification Using RSA Based-PDP (RSA-PDP) in Multi Cloud Storage. *Excel International Journal of Technology, Engineering and Management, 2*(1), 10-13.

[43] Senthilkumar, V., & Prashanth, K. (2016). A Survey of Rendezvous Planning Algorithms for Wireless Sensor Networks. *International Journal of Communication and Computer Technologies, 4*(1), 29-34.

[44] Dr.Sundararaju, K., & Rajesh, T. (2016). Control Analysis of Statcom under Power System Faults. *International Journal of Communication and Computer Technologies, 4*(1), 46-50.

[45] Ban Maheskumar N., & Prof.Sayed Akhtar, H. (2016). An online and offline Character Recognition Using Image Processing Methods-A Survey. *International Journal of Communication and Computer Technologies, 4*(2), 102-107.

[46] Chaharboor, M., Mokhtabad, S., & Ghonoodi, H. (2016). New approach of constructing ADPLL by a novel Quadrature Ring Oscillator using Low-Q Series LC tanks. *International Academic Journal of Science and Engineering, 3*(4), 44-60.

[47] Rahin, V.B., & Rahin, A.B. (2016). A Low-Voltage and Low-Power Two-Stage Operational Amplifier Using FinFET Transistors. *International Academic Journal of Science and Engineering, 3*(4), 80-95.

[48] Roein, M.A., & Golmakani, A. (2016). A low power and high gain CMOS LNA for UWB applications using a gate inductor. *International Academic Journal of Science and Engineering, 3*(4), 122-131.

[49] Aswini, P., & amala Kannan, T. K. (2015).Barcode Reading using Mobile in Web Application for Dispatch Management. *International Scientific Journal on Science Engineering & Technology, 18*(6), 134-137.

[50] Dr. Sujatha, P., & Kanimozhi (2015).An Evolution of Big Data and its Challenges. *International Scientific Journal on Science Engineering & Technology, 18*(6), 138-141.