isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

Detect Packet Droppers And Modifiers Using Light Weight Secure Scheme

K.V.Sridevi[1],P.Yamini priyanka[2],Mrs.A. Beenagodbin[3]

Student, Department of Computer Science and Engineering,

Agni College of Technology, India[1,2]

Asst. Professor, Dept. of Computer Science and Engineering,

Agni College of Technology, India[3]

Abstract:

Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information.A malicious adversary may introduce additional nodes in the network or compromise existing ones.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 aBase station (BS) that performs decision-making. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. This propose a novel lightweight scheme to securely transmit provenance for sensor data. It introduces efficient mechanisms for provenance verification and reconstruction at the base station. And this, extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs.

Keywords: Provenance, Security, Sensor networks

1.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.

2.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. This system also does not address security concerns and is specific to some network use cases. SNP extends network provenance to adversarial environments. Since all of these systems are general purpose network provenance systems, they are not optimized for the resource constrained sensor networks. It proposes a chain model of provenance and ensures integrity and confidentiality through encryption, checksum and incremental chained signature mechanism. It extends this method by applying digital signatures to a DAG model of provenance. However, these generic solutions are not aware of the sensor network specific assumptions, constraints, etc.

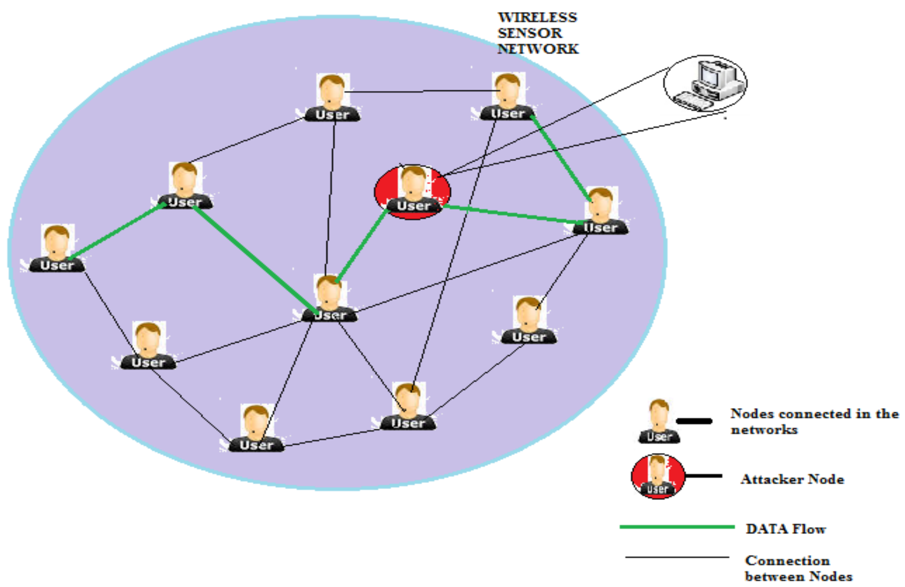
This system traces the source of a stream long after the process has completed. It reflects the importance of issues we addressed, it is not intended as a security mechanism, hence, does not deal with malicious attacks.

3.PROPOSED SYSTEM:

We propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce 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. It proposes an in-packet Bloom filter (iBF) provenance-encoding scheme. The problem of secure provenance transmission in sensor networks, and identifies the challenges specific to this context, the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes. 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. A multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. 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.

Consider a Wireless sensor networks with large number of user nodes ,which are homogeneous in functionalities and capabilities. We assume that the Base Station (BS) is always reliable. In the network any of the sensor node may be compromised by attackers and the data transmission may be interrupted from attacks on a wireless channel .Hence the monitor sensors senses the attacker node and blocks the attacker .The monitor sensor sends an acknowledgment to the base station for the retransmission of data ,in order to send the data to its destination.

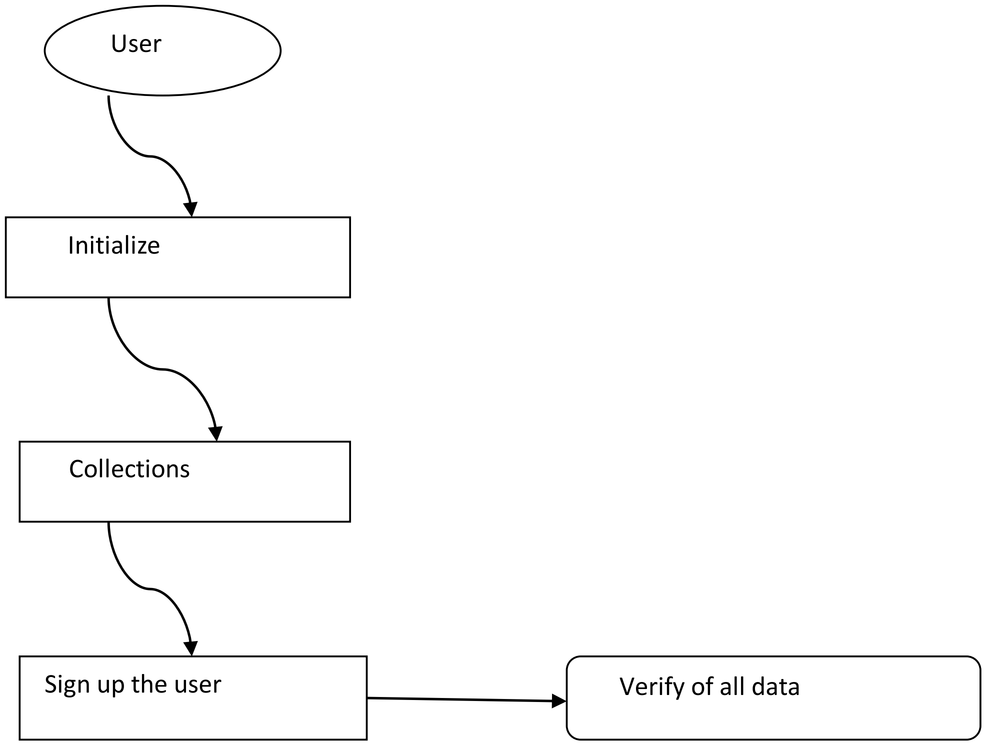
4.SYSTEM ARCHITECTURE:



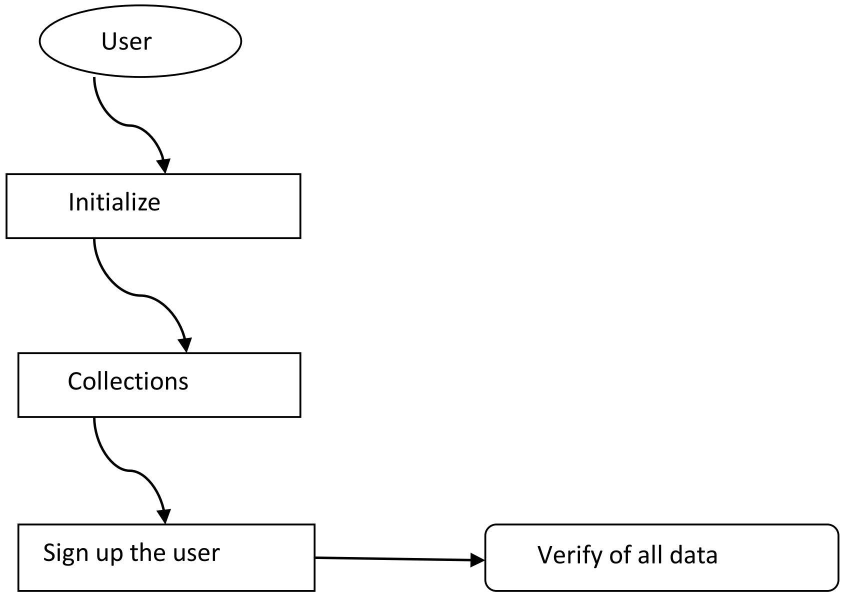
4.1Provenance Verification:

In verify modules it process the Key generation, decryption, key exchanging, send to receiver module. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated. In Provenance Collection, receiver module receives a packet data suspicious means place in suspicious box suppose data correct data means placed in province box. The BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance.

PROVENANCE IDENTIFICATION:



DATA VERIFICATION:

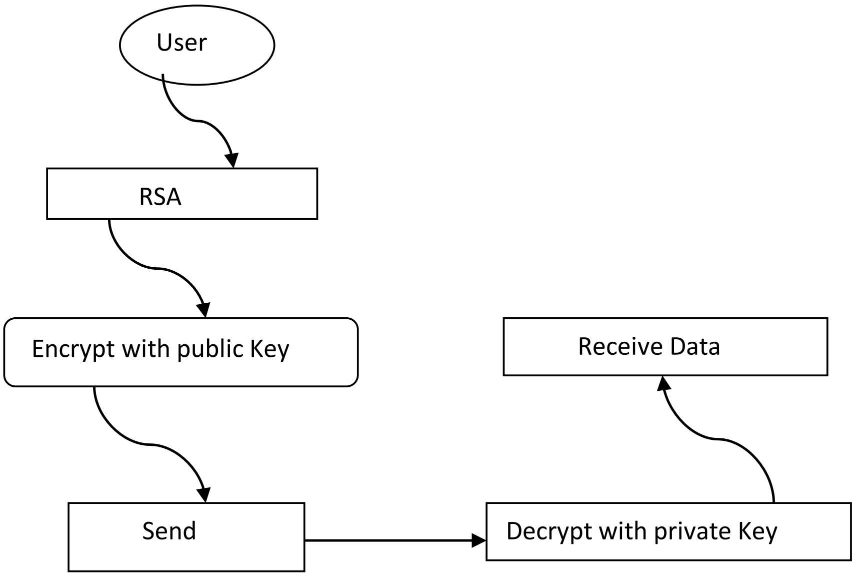


5

4.2Provenance Encoding and Decoding:

In provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node. For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF. Each vertex originates at a node in the data path and represents the provenance record of the host node. A vertex is uniquely identified by the vertex ID. When the BS receives a data packet, it executes the provenance verification process, which assumes that the BS knows what the data path should be, and checks the iBF to see whether the correct path has been followed. However, right after network deployment, as well as when the topology changes (e.g., due to node failure), the path of a packet sent by a source may not be known to the BS. In this case, a provenance collection process is necessary, which retrieves provenance from the received iBF and thus the BS learns the data path from a source node.

Provenance Encoding and Decoding:



4.3 Data Provenance:

Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission.

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

5.CONCLUSION:

We 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 scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable.

5.1FUTURE:

In future work, we plan to implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

1. Salmin Sultana, Gabriel Ghinita, Elisa Bertino"A Lightweight Secure Provenance for Wirelesss Sensor Network IEEE 2012 18th International Conference on parallel and distribution system.

2. Yogesh L.Simmhan, Beth Plale,Dennis Gannon “A Survey of data Provrence in e-Science” Sigmoid Record Vol. 34,no.3, Sept 2005.

3. Koustuv Dasgupta, Konstantinos Kalpakis And Parag Namjoshi "An. efficient clustering based heuristic for data gathering in sensor network " IEEE 2003.

4. Christian Esteve Rothenberg, Carlos A.B.Macapuna “In -packet Bloom Filters :Design and Networking Application” 20th Jan 2010.

5. Salmin Sultana, Mohamed Shehab, Elisa Bertino “Secure Provenance Transmission for Streaming Data” IEEE 2012.

6. T. Hara,V. I. Zadorozhny and E.Buchmann,Wireless Sensor Network Technologies for the Information Explosion Era,Stud.Comput.Intell.Springer,Verlag,2010,vol.278.

7. Y.Wang,G.Attebury and B.Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Commun.Surveys Tuts.,vol 8,no. 2,pp.2-23,2006.

8. K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, “Provenance-Aware Storage systems”