South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 73–80

**ISSN No: 2454-9614**

# An Integrated Security Solution for Data Distribution in WSN

T. Janaranjaniaani, P. Balamurugan*, V. Sharmila

*Department of Computer Science and Engineering, K.S.R College of Engineering, Namakkal, Tamil nadu, India.*

*Corresponding Author: T.Janaranjanil,

E-mail: theerkapalaniswamyse@gmail.com

**Received: 08/11/2015, Revised: 12/11/2015 and Accepted: 03/03/2016**

**Abstract:**

Environment monitoring is achieved using the sensor devices. Sensor device manages the sense, update and transmit operations. Pressure, temperature and humidity information's are observed by the sensor devices. Energy and bandwidth limitations are considered in the sensor network applications. Sensor network data distribution process is violated by the intruders. Anonymous data packets are inserted by the malicious nodes. Data verification methods are applied to identify the malicious data packets. Base station manages the sensor node data transmission process through the path nodes. Sensor data are verified with the support of provenance verification scheme. Power consumption, bandwidth, storage space and security parameters are considered in the data distribution process. Sensor data responses are validated using the secure provenance verification scheme. Data verification details are encoded with In packet Bloom filters (iBF). Base station handles the provenance verification tasks. Packet drop attacks are also detected by the security scheme. The data distribution process is performed with Provenance collection algorithm. The data verification scheme is improved with continuous malicious node attacks. Node and data verification schemes are integrated in the system. Node level trust verification is performed with distributed trust model. Node properties are used in the **node** level trust verification process. The sensor data distribution is carried out with authentication, confidentiality and integrity methods.

**Reviewed by* **ICETSET'16** *organizing committee*

## 1. Introduction

Wireless sensor network (WSN) is deployed there is usually a need to update buggy/old small programs or parameters stored in the sensor nodes. This can be achieved by the so-called data discovery and dissemination protocol, which facilitates a source to inject small programs, commands, queries and configuration parameters to sensor nodes. Note that it is different from the code dissemination protocols, which distribute large binaries to reprogram the whole network of sensors. For example, efficiently disseminating a binary file of tens of kilobytes requires a code dissemination protocol while disseminating several 2-byte configuration parameters requires data discovery and dissemination protocol. Considering the sensor nodes could be distributed in a harsh environment, remotely disseminating such small data to the sensor nodes through the wireless channel is a more preferred and practical approach than manual intervention.

In the literature, several data discovery and dissemination protocols have been proposed for WSNs. Among them, DHV, DIP and Drip are regarded as the state-of-the-art protocols and have been included in the Tiny OS distributions. All proposed protocols assume that the operating environment of the WSN is trustworthy and has no adversary. Adversaries exist and impose threats to the normal operation of WSNs. This issue has only been addressed recently by **[7]** identifies the security vulnerabilities of Drip and proposes an effective solution.

More importantly, all existing data discovery and dissemination protocols employ the centralized approach data items can only be disseminated by the base station. Unfortunately, this approach suffers from the single point of failure as dissemination is impossible when the base station is not functioning or when the connection between the base station and a node is broken. In addition, the centralized approach is inefficient, non-scalable, and vulnerable to security attacks that can be launched anywhere along the communication path **[2].** Even worse, some WSNs do not have any base station at all. For example, for a WSN monitoring human trafficking in a country's border or a WSN deployed in a remote area to monitor illicit crop cultivation, a base station becomes an attractive target to be attacked. For such networks, data dissemination is better to be carried out by authorized network users in a distributed manner.

Additionally, distributed data discovery and dissemination is an increasingly relevant matter in WSNs, especially in the emergent context of shared sensor networks, where sensing/communication infrastructures from multiple owners will be shared by applications from multiple users. For example, large scale sensor networks are built in recent projects such as Geoss, NOPP and ORION. These networks are owned by multiple owners and used by various authorized third-party users. It is expected that network owners and different users may have different privileges of dissemination. In this context, distributed operation by networks owners and users with different privileges will be a crucial issue, for which efficient solutions are still missing.

## 2. Related Work

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al. and Agrawal et al. **[8]** proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Diffie-Hellman (DH), respectively. Both schemes are not suited for sensors with limited resources and are unable to perform expensive computations with large key sizes. Since ECC is computationally more efficient and has a short key length, several approaches with certificate **[3]** have been proposed based on ECC.

Since each node must exchange the certificate to establish the pairwise key and verify each other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Existing schemes **[10]** are not secure. Alagheband et al. **[5]** proposed a key management scheme by using ECC-based signcryption, but this scheme is insecure against message forgery attacks **[6].** Huang et al. proposed a ECC-based key establishment scheme for self-organizing

WSNs. We found the security weaknesses of their scheme. In step 2 of their scheme, a sensor node *U* sends *z = qU · H(MacKey) + dU (modn)* to the other node *V* for authentication, where *qU* is a static private key of *U*. But, once *V* receives the *z*, it can disclose *qU*, because *V* already got *MacKey* and *dU* in step 1. So, *V* can easily obtain *qU* by computing *qU = (z − dU) · H(MacKey)* −1. Thus, the sensor node's private key is exposed to the other node during the key establishment between two nodes. Zhang et al. **[10]** proposed a distributed deterministic key management scheme based on ECC for dynamic WSNs.

It uses the symmetric key approach for sharing the pairwise key for existing nodes and uses an asymmetric key approach to share the pairwise keys for a new node after deployment. Since the initial key *KI* is used to compute the individual keys and the pairwise keys after deployment for all nodes, if an adversary obtains *KI*, the adversary has the ability to compute all individual keys and the pairwise keys for all nodes. Also, since such scheme uses a simple ECC-based DH key agreement by using each node's long-term public key and private key, the shared pairwise key is static and as a result, is not secure against known-key attacks and cannot provide re-key operation. Du et al. **[3]** use an ECDSA scheme to verify the identity of a cluster head and a static EC-Diffie-Hellman key agreement scheme to share the pairwise key between the cluster heads. The scheme by Du et al. is not secure against known-key attacks, because the pairwise key between the cluster heads is static. Du et al. use a modular arithmetic-based symmetric key approach to share the pairwise key between a sensor node and a cluster head. The scheme does not provide a process to protect against clone and impersonation attack. Rahman et al. **[4]** and Chatterjee et al. **[9]** have proposed ID PKC based key management schemes supporting the mobility of nodes in dynamic WSNs which removes the certificate management overhead. Their schemes require expensive pairing operations. Although many approaches that enable pairing operations for sensor nodes have been proposed, the computational cost required for pairing is still considerably higher than standard operations such as ECC point multiplication. For example, NanoECC, which uses the MIRACL library, takes around 17.93s to compute one pairing operation and around 1.27s to compute one ECC point multiplication on the MICA2 mote.

## 3. Distributed Trust and Provenance Models for WSN

### *3.1. Sensor Trust Analysis*

WSNS are emerging technologies that have been widely used in many applications such as emergency response, healthcare monitoring, battlefield surveillance, habitat monitoring, traffic management, smart power grid **[1],** etc. The wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Providing security is extremely important for the safe application of WSNs.

Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. These approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we

need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node.

Many researchers have developed trust models to build up trust relationships among sensor nodes **[11].** For example, a distributed Reputation-based Framework for Sensor Networks (RFSN) is first proposed for WSNs. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is responsible for monitoring communication behaviours of neighbour nodes. Reputation System is responsible for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. In RFSN, only the direct trust is calculated while the recommendation trust is ignored. A Parameterized and Localized trUst management Scheme (PLUS). In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node receives a packet from suspect node, it always checks the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviours or not. Suspect node may get unfair penalty. Another similar trust evaluation algorithm named as Node Behavioural strategies banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed based on behaviour strategy banding D-S belief theory **[12].** NBBTE algorithm first establishes various trust factors depending on the communication behaviours between two neighbour nodes. Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbour nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one. To the best of our knowledge, NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviours to evaluate the trustworthiness of sensor nodes. Therefore, NBBTE is chosen as the comparing algorithm in this paper.

*3.2. Provenance Verification Scheme*

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. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures. Although provenance modelling, collection, and querying have been studied extensively for workflows and curate databases, provenance in sensor networks has not been properly addressed. We investigate the problem of secure and efficient provenance transmission and processing for sensor networks and we use provenance to detect packet loss attacks staged by malicious sensor nodes.

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. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Furthermore, sensors often operate in an untrusted environment,

where they may be subject to attacks. 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. We propose a 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.

As opposed to existing research that employs separate transmission channels for data and provenance, we only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, we use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice.

*3.3. Issues on Sensor Node Security*

Sensor data are streamed from multiple sources through intermediate processing nodes. Data provenance is applied to evaluate the trustworthiness of sensor data. Low energy and bandwidth consumption, efficient storage and secure transmission factors are considered in provenance management. Secure provenance verification scheme is used to authorize sensor data packets. In packet Bloom filters (iBF) are used to encode provenance. Provenance verification and reconstruction tasks are carried out under the base station. Secure provenance scheme is extended with functionality to detect packet drop attacks. Provenance collection algorithm and provenance verification algorithm are used in the data verification process. The following drawbacks are identified from the existing system. Multiple consecutive malicious sensor nodes based attacks are not handled. Packet lose detection accuracy is low. Node level trust factors are not considered. Time bounded provenance verification is not supported.

## 4. Data Verification Requirements

We assume that the BS is trusted, but any other arbitrary node may be malicious. An adversary can eavesdrop. Provenance graph for a sensor network. Perform traffic analysis anywhere on the path. In addition, the adversary is able to deploy a few malicious nodes, as well as compromise a few legitimate nodes by capturing them and physically overwriting their memory. If an adversary compromises a node, it can extract all key materials, data, and codes stored on that node. The adversary may drop, inject or alter packets on the links that are under its control **[13].** We do 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 BS. Instead, the primary concern is that an attacker attempts to misrepresent the data provenance. Our objective is to achieve the following security properties:

- Confidentiality. An adversary cannot gain any knowledge about data provenance by analyzing the contents of a packet. Only authorized parties can process and check the integrity of provenance.

- Integrity. An adversary, acting alone or colluding with others, cannot add or remove non-colluding nodes from the provenance of benign data without being detected.
- Freshness. An adversary cannot replay captured data and provenance without being detected by the BS.
- 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.

**5. Secured Data Distribution in WSN**

The secure provenance verification scheme is enhanced to handle consecutive malicious node attacks. Efficient Distributed Trust Model (EDTM) is improved with security features. Integrated verification scheme is designed to authorize the node and data. Coordinated trust model is constructed with communication, energy, data and recommendation trust values.

The sensor network security system is designed to manage node and data verification operations. Anonymous data and malicious data forwarding operations are controlled by the system. Trust verification is performed to ensure network level security. The system divided into six major modules. They are Base Station, Provenance Management, Trust Assignment, Data Verification, Node Verification and Attack Handler. The base station is deployed to manage the wireless sensor network. Provenance management module handles the provenance release operations. Node level trust values are estimated under trust assignment module. Provenance verification is carried out under the data verification process. Node verification is performed with trust details. Packet dropping attacks are managed under attack handler.

The base station manages the sensor nodes in WSN. Sensor nodes and their properties are maintained under the base station. Authentication and verification operations are carried out under base station. Data request operations are initiated from the base station. The base station releases the provenance for each node. Sensor data trust is ensured with data provenance. Provenance is encoded with in packet Bloom filters (iBF) data structures. Provenance graph is constructed with node information.

Reliability, utility, availability, risk and quality of services factors are considered in the trust assignment process, Trust assignment is performed with coordinated trust model, each node is assigned with four trust values, Communication, energy, data and recommendation trust values are used in the system. Secure provenance verification scheme is adapted to carry out the data verification process, Provenance collection algorithm is used to identify the presence of a node in provenance graph, Provenance and its integrity are checked using the provenance verification algorithm, The provenance verification process is enhanced with time bounded model. Node verification is performed with Efficient Distributed Trust Model (EDTM). Trust values are used to verify the belief of a node. EDTM uses one hop trust model and multi hop trust model for the node verification process. Security features are integrated with the EDTM scheme.

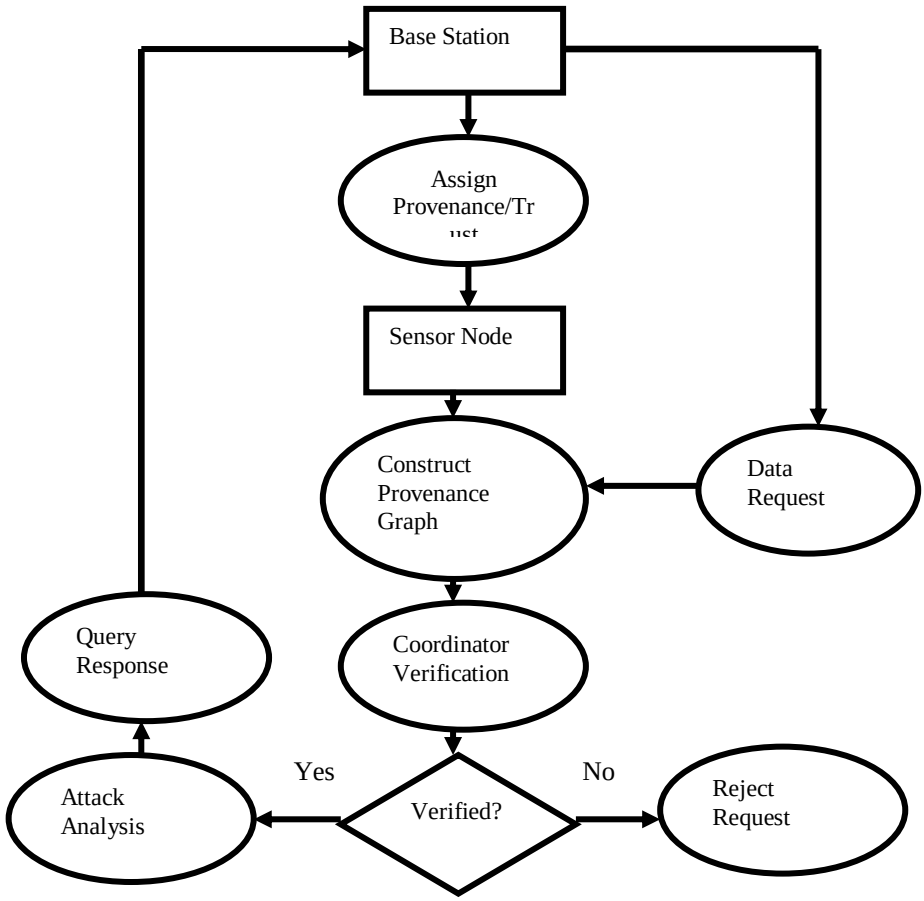


Figure 5.1 Secured Data Distribution Scheme

Packet dropping attacks and malicious data forwarding attacks are detected under attack handler. Acknowledgement with sequence number is verified to identify the packet drop attacks. The system also detects multiple consecutive malicious sensor nodes based attacks. Path changes are suggested.

**6. Conclusion**

Sensor node data values are transferred through multi hop data transmission models. Secure provenance verification schemes are used to authorize the data packets. Efficient Distributed Trust Model (EDTM) is integrated with provenance verification scheme for node and data level trust analysis. Packet drop attack detection process is improved with time bounded verification mechanism. The system integrates the node and data verification operations in the wireless sensor networks. Multi trust model based node verification mechanism is applied in the request and response operations. Energy and traffic levels are reduced in the data transmission process. The system ensures reliable data delivery with minimum delay.

## References

[1] V. C. Gungor, L. Bin and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, Oct. 2010.
[2] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012.
[3] D. Du, H. Xiong and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.
[4] M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, 2010.
[5] M. Alagheband and M. R. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, 2012.
[6] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.
[7] D. He, S. Chan, S. Tang and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638–4646, Sep. 2013.
[8] S. Agrawal, R. Roman, M. L. Das, A. Mathuria and J. Lopez, "A novel key update protocol in mobile sensor networks," in Proc. 8th Int. Conf. ICISS, vol. 7671. 2012.
[9] K. Chatterjee, A. De, and D. Gupta, "An improved ID-based key management scheme in wireless sensor network," in Proc. 3rd Int. Conf. ICSI, vol. 7332. 2012, pp. 351–359.
[10] X. Zhang, J. He and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.
[11] G. Han, J. Jiang, L. Shu, J. Niu and H. C. Chao, "Managements and applications of trust in wireless sensor networks: A Survey," J. Comput. Syst. Sci., vol. 80, no. 3, 2014.
[12] R. Feng, X. Xu, X. Zhou and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory," Sensors, vol. 11, 2011.
[13] Seung-Hyun Seo and Elisa Bertino, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 2, February 2015.