International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 12
August 2016

Data Confidentiality in Secure and Distributed Data Discovery and Dissemination Protocols in WSNs

M.Raghavendra[1], Dr.M.Nagendra[2]
[1]Ph.D Scholor, Department of Computer Science and Technology, Sri Krishnadevaraya University
[2]Professor, Department of Computer Science and Technology, Sri Krishnadevaraya University

Abstract:

Wireless sensor networks (WSN) are basically distributed networks or a collection of sensor nodes which collect information which are used to analyse physical or environmental conditions. WSNs are usually setup in remote and hostile areas and work in extreme conditions. Applications of WSN include habitat monitoring, industrial applications, battlefield surveillance, smart homes etc. Most of them require regular updating of software in sensor nodes through the wireless channel for efficient management and working. So it is necessary to spread data through the wireless medium after the nodes are deployed. This is known as data dissemination. A data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. All existing data discovery and dissemination protocols suffer from two drawbacks. First, they are based on the centralized approach; only the base station can distribute data items. Such an approach is not suitable for emergent multi-owner-multi-user WSNs. Second, those protocols were not designed with security in mind and hence adversaries can easily launch attacks to harm the network. This paper proposes the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. We are also providing data confidentiality in the design of secure and distributed data discovery and dissemination protocols.

1.INTRODUCTION

Wireless Sensor Networks (WSN) is one of the major milestones in the field of communication. These networked collection of nodes take us a step closer to obtaining valuable information about the physical world. WSN are used popularly in many applications like remote control and monitoring, construction safety systems, environmental monitoring, health care management, disaster management, surveillance operations, smart homes, habitat monitoring, indoor sensor networks, seismic monitoring of buildings etc [1]. In computer science and communication wireless sensor networks entertain lot of research today.

A WSN is made of sensor nodes used for monitoring and analysis purposes as shown in Fig 1. These sensor nodes pass the information that they collect to a prime location called a base station. In most systems, a WSN communicates with a LAN or WAN through a gateway like medium. The gateway is actually a bridge between the WSN and the various other networks [2]. This allows data to be stored by devices and which can be taken up for processing later. Each sensor node or mote has several parts: a circuit for interfacing with other sensor nodes, a micro controller, a radio transceiver, and a battery for power supply. The topology used can be either a star, ring, grid network or multi-hop wireless mesh network.WSN is used primarily in remote and hostile environments for information collection. Hence it is a major challenge to produce cheap sensor nodes. They must be designed carefully by considering all the different constraints of the environment in consideration.

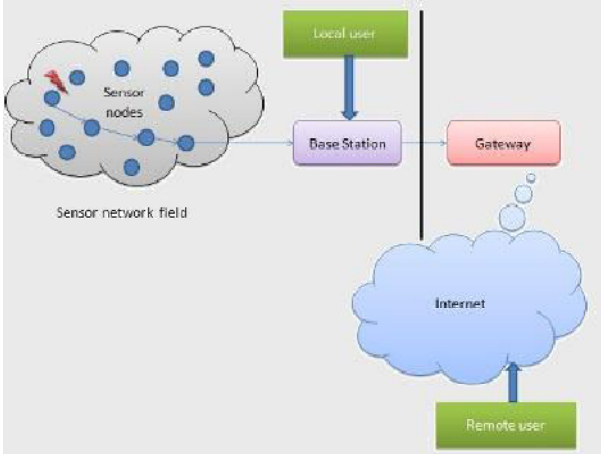

Fig -1: An example wireless sensor network

Wireless sensor networks must be operated for long duration of time and usually don't get any human administration or intervention in between [3].

In the literature, several data discovery and dissemination protocols [4], [5], [6], [7] have been proposed for WSNs.
Among them, DHV [4], DIP [6] and Drip [5] are regarded as the state-of-the-art protocols and have been included in the TinyOS distributions. All proposed protocols assume that the operating environment of the WSN is trustworthy and has no adversary. However, in reality, adversaries exist and impose threats to the normal operation of WSNs [8], [9]. This issue has only been addressed recently by [8] which identifies the security vulnerabilities of Drip and proposes an effective solution. More importantly, all existing data discovery and dissemination protocols [4], [5], [6], [7], [8] employ the centralized approach in which, as shown in the top sub-figure in Fig. 2, 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. 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 [10], NOPP [11] and ORION [12]. These networks are owned by multiple owners and used by various authorized third-party users. Moreover, 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.
Motivated by the above observations, this paper has the following main contributions:
1) The need of distributed data discovery and dissemination protocols is not completely new, but previous work did not address this need. We study the functional requirements of such protocols, and set their design objectives. Also, we identify the security vulnerabilities in previously proposed protocols.
2) Based on the design objectives, we propose DiDrip. It is the first distributed data discovery and dissemination protocol, which allows network owners and authorized users to disseminate data items into WSNs without relying on the base station. Moreover, our extensive analysis demonstrates that DiDrip satisfies the security requirements of the protocols of its kind. In particular, we apply the provable security technique to formally prove the authenticity and integrity of the disseminated data items in DiDrip.
3) We demonstrate the efficiency of DiDrip in practice by implementing it in an experimental WSN with resource-limited sensor nodes. This is also the first implementation of a secure and distributed data discovery and dissemination protocol.

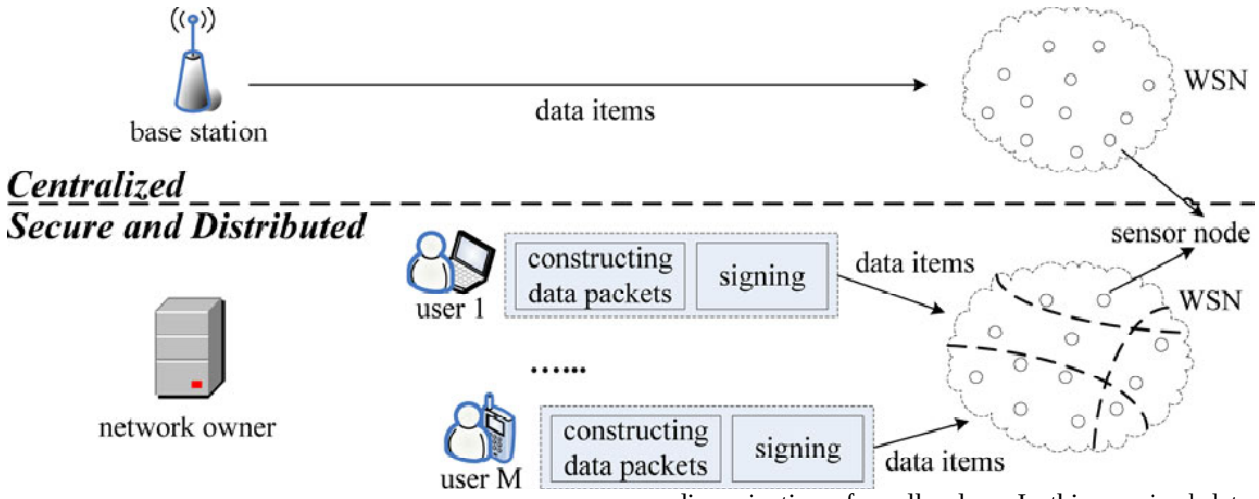

Fig2: System overview of centralized and distributed data discovery and dissemination approaches.

The rest of this paper is structured as follows. In Section 2, we first survey the existing data discovery and dissemination protocols, and then discuss their security weaknesses. Section 3 describes the requirements for a secure and distributed extension of such protocols.

2. SURVEY AND SECURITY VULNERABILITIES IN DATA DISCOVERY AND DISSEMINATION

2.1 Review of Existing Protocols

A. Drip

The sensor network management systems dissemination protocol named Drip protocol was proposed by Tolle et al.[13]. This is the simplest of all dissemination protocols which uses trickle algorithm. For transmitting of a new message, a new version number is generated and used. This will cause the protocol to reset the Trickle timer and thus disseminate the new value. It has a standard message reception interface. Each node gets registered with the specific identifier, which represents a dissemination channel. The messages received are delivered to the node directly. Recent messages are broadcasted quickly All messages received on that channel will be delivered directly to the node. Drip avoids redundant transmission and achieves greater efficiency.

B. Code Drip

This data dissemination protocol proposed by Nildo et al.[14] uses network coding and is mainly used for dissemination of small values. In this, received data packets are combined by sensor nodes to one packet and this combined packet is sent to its neighbours. It uses trickle algorithm. Network Coding is a mechanism that combines packets in the network thus increasing the throughput and decreasing number of messages transmitted and also improves reliability and speed of dissemination.

C. SeDrip

Daojing He et al. proposed a secure, lightweight, and Denial-of Service (DoS)-resistant data discovery and dissemination protocol named SeDrip. SeDrip protocol works under limited resources of sensor nodes. The ECC public key algorithm and Merkle hash tree is combined in SeDrip to avoid frequent public key operations and achieve strong robustness against various malicious attacks.

SeDrip consists of three phases: system initialization, packet pre-processing, and packet verification. Se-drip suffers from some disadvantages, that is delay and centralised approach.

D. DiDrip

Distributed data discovery and dissemination protocol [15] was proposed to overcome the disadvantages of SeDrip. It consists of four phases they are System Initialization Phase, User- Joining Phase, Packet Pre-Processing phase and Packet Verification phase. Few Sensor nodes are considered as network owner and few as users and one node as destination. ECC cryptography is used for key generation and keys are distributed to all nodes. Hash function is used to make it more secure. DiDrip is implemented by using two methods they are data hash chain and Merkle hash tree method.

E. DIP

Dissemination Protocol (DIP) is a data detection and dissemination protocol proposed by Lin et al. [16].

This protocol is based on Trickle algorithm. It Detects difference of data in a node and identifies the different data item .The concept of version number and keys for each data item is followed . In addition to the version number, DIP ensures that all nodes have same data by decrementing hashes to a minimum of 0.

F. MNP

Sandeep et al. proposed a multihop network reprogramming protocol (MNP) [17]. It provides a Reliable service to propagate new program code to all sensor nodes in the network. The main aim of this dissemination protocol is to ensure reliable, low memory usage and fast data dissemination. It is based on a sender selection protocol in which source nodes compete with each other based on the number of distinct requests they have received. In each neighbourhood, a source node sends out program codes to multiple receivers. When the receivers get the full program image at their side, they become source nodes, and send the code into their neighbourhood. Issues of collisions exists. This is solved by selecting a suitable sensor node based on some parameters maintained by the nodes and some advertisement and download messages exchanged by the nodes. It is like a greedy algorithm. Pipelining can be included in this protocol to enable faster data propagation in the case of larger networks.

G. DHV

It is a code consistency maintenance protocol (Difference detection, Horizontal search, and Vertical search).given by Dang et al. [18]. It tries to keep codes on different nodes in a WSN consistent and up to date. The data items are represented as tuples (key, version).This protocol tries to overcome the disadvantages of previous protocols like DRIP and DIP by reducing the complexity involved in the updating of data in the network. It is based on the observation that if two versions are different, they may only differ in a few least significant bits of their version number rather than in all their bits. Hence, it is not always necessary to transmit and compare the whole version number in the network. Here the version number is given as a bit array. DHV uses bit slicing to quickly determine the out of date code, resulting in fewer bits being transmitted in the network.

2.2 Security Vulnerabilities

An adversary can first place some intruder nodes in the network and then use them to alter the data being disseminated or forge a data item. This may result in some important parameters being erased or the entire network being rebooted with wrong data. For example, consider a new data item (key, version, data) being disseminated. When an intruder node receives this new data item, it can broadcast a malicious data item (key, version_, data_), where version_ > version. If data_ is set to 0, the parameter identified by key will be erased from all sensor nodes. Alternatively, if data_ is different from data, all sensor nodes will update the parameter according to this forged data item. Note that the above attacks can also be launched if an adversary compromises some nodes and has access to their key materials.

In addition, since nodes executing Trickle are required to forward all new data items that they receive, an adversary can launch denial-of-service (DoS) attacks to sensor nodes by injecting a large amount of bogus data items. As a result, the processing and energy resources of nodes are expended to process and forward these bogus data items, rather than on the intended functions. Any data discovery and dissemination protocol based on Trickle or its variants is vulnerable to such a DoS attack.

3 REQUIREMENTS AND DESIGN CONSIDERATION

A secure and distributed data discovery and dissemination protocol should satisfy the following requirements:

1) Distributed. Multiple authorized users should be allowed to simultaneously disseminate data items into the WSN without relying on the base station.

2) Supporting different user privileges. To provide flexibility, each user may be assigned a certain privilege level by the network owner. For example, a user can only disseminate data items to a set of sensor nodes with specific identities and/or in a specific localized area. Another example is that a user just has the privilege to disseminate data items identified by some specific keys.

3) Authenticity and integrity of data items. A sensor node only accepts data items disseminated by authorized users. Also, a sensor should be able to ensure that received data items have not been modified during the dissemination process.

4) User accountability. User accountability must be provided since bad user behaviors and insider attacks should be audited and pinpointed. That is, a sender should not be able to deny the distribution of a data item. At the same time, an adversary cannot impersonate any legitimate user even if it has compromised the network owner or the other

legitimate users. In many applications, accountability is desirable as it enables collection of users' activities. For example, from the dissemination record in sensor nodes, the network owner can find out who disseminates most data. This requires the sensor nodes to be able to associate each disseminated data with the corresponding user's identity.

5) Node compromise tolerance. The protocol should be resilient to node compromise attack no matter how many nodes have been compromised, as long as the subset of non-compromised nodes can still form a connected graph with the trusted source.

6) User collusion tolerance. Even if an adversary has compromised some users, a benign node should not grant the adversary any privilege level beyond that of the compromised users.

7) DoS attacks resistance. The functions of the WSN should not be disrupted by DoS attacks.

8) Freshness. A node should be able to differentiate whether an incoming data item is the newest version.

9) Low energy overhead. Most sensor nodes have limited resources. Thus, it is very important that the security functions incur low energy overhead, which can be decomposed to communication and computation overhead.

10) Scalability. The protocol should be efficient even for large-scale WSNs with thousands of sensors and large user population.

11) Dynamic participation. New sensor nodes and users can be dynamically added to the network.In order to ensure security, each step of the existing data discovery and dissemination protocol runs should be identified and then protected. In other words, although code dissemination protocols may share the same security requirements as listed above, their security solutions need to be designed in accordance with their characteristics. Considering the well known open-source code dissemination protocol Deluge as an example. Deluge uses an epidemic protocol based on a page-by-page dissemination strategy for efficient advertisement of metadata. A code image is divided into fixed-size pages, and each page is further split into same-size packets. Due to such a way of decomposing code images into packets, our proposed protocol is not applicable for securing Deluge.

The primary challenge of providing security functions in WSNs is the limited capabilities of sensor nodes in terms of computation, energy and storage. For example, to provide authentication function to disseminated data, a commonly used solution is digital signature. That is, users digitally sign each packet individually and nodes need to verify the signature before processing it. However, such an asymmetric mechanism incurs significant computational and communication overhead and is not applicable to sensor nodes. To address this problem, TESLA and its various extensions have been proposed [13], [14], which are based on the delayed disclosure of authentication keys, i.e., the key used to authenticate a message is disclosed in the next message.

Unfortunately, due to the authentication delay, these mechanisms are vulnerable to a flooding attack which causes each sensor node to buffer all forged data items until the disclosed key is received. Another possible approach to authentication is by symmetric key cryptography. However, this approach is vulnerable to node compromise attack because once a node is compromised, the globally shared secret keys are revealed. Here we choose digital signatures over other forms for update packet authentication. That is, the network owner assigns to each network user a public/private key pair that allows the user to digitally sign data items and thus authenticates himself/herself to the sensor nodes. We propose two hybrid approaches to reduce the computation and communication cost. These methods combine digital signature with efficient data Merkle hash tree and data hash chain, respectively.

The main idea is that signature generation and verification are carried out over multiple packets instead of individual packet. In this way, the computation cost per packet is significantly reduced. Since elliptic curve cryptography (ECC) is computational and communication efficient compared with the traditional public key cryptography, DiDrip is based on ECC. To prevent the network owner from impersonating users, user certificates are issued by a certificate authority of a public key infrastructure (PKI), e.g., local police office.

4.CONCLUSION

In this paper, we have identified the security vulnerabilities in data discovery and dissemination when used in WSNs, which have not been addressed in previous research. Also, none of those approaches support distributed operation. Therefore, in this paper, a secure and distributed data discovery and dissemination protocol named DiDrip has been proposed.

5.REFERENCES

[1] Mohammad A. Matin, Wireless Sensor Networks: Technology and Protocols: Published by InTech, Croatia, ISBN 978-953-51-0735-4, 2012.

[2] Salvatore La Malfa, Wireless Sensor Networks, 2010.

[3] Jisha Mary Jose, Jomina John, "Data dissemination protocols in wireless sensor networks-a survey", IJARCCE, March 2014.

[4] T.Dang,N. Bulusu,W. Feng, and S. Park, "DHV:Acode consistency
maintenance protocol for multi-hop wireless sensor networks," in
Proc. 6th Eur. Conf.Wireless Sensor Netw., 2009, pp. 327–342.

[5] G. Tolle and D. Culler, "Design of an application-cooperative
management system for wireless sensor networks," in Proc. Eur.
Conf. Wireless Sensor Netw., 2005, pp. 121–132.

[6] K. Lin and P. Levis, "Data discovery and dissemination with
DIP," in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008,
pp. 433–444.

[7] M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M.
Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildings
with wireless sensor networks: The Torre Aquila deployment," in
Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

[8] 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.

[9] M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing
synchronization for heterogeneous sensor networks," in Proc.
IEEE Global Telecommun. Conf., 2008, pp. 1–5.

[10] Geoss. [Online]. Available: http://www.epa.gov/geoss/

[11] NOPP. [Online]. Available: http://www.nopp.org/

[12] ORION. [Online]. Available: http://www.joiscience.org/ocean observing/advisors

[13] G. Tolle and D. Culler , "Design of an application-cooperative management system for wireless sensor networks", in Proc. EWSN, pp. 121–132, 2005.

[14] NildoRibeiro Junior, Marcos A. M. Vieira, Luiz F. M. Vieira, and Omprakash Gnawali,"CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks", in Proceedings of the 11th European conference on Wireless sensor networks (EWSN 2014), Feb. 2014.

[15] A.SenthilKumar,S.Velmurugan,E.Logashanmugam." A secure distributed data discovery and dissemination in wireless sensor networks", International Journal of Engineering & Science Research, ISSN 2277-2685 Vol-5,Issue-7,708-713, July 2015

[16] Lin, K., Levis, P.," Data discovery and dissemination with DIP", In :Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008), Washington, DC,USA, IEEE Computer Society (2008) 433–444.

[17] S. Kulkarni and L. Wang,."Mnp: Multihop network reprogramming service for sensor network". In 25th International Conference on Distributed Computing Systems, June 2005.

[18] T. Dang, N. Bulusu, W. Feng, and S. Park, "DHV: a code consistency maintenance protocol for multi-hop wireless sensor networks," in Proc. 2009 EWSN, pp. 327–342.

[13] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure
source authentication for multicast," in Proc. Netw. Distrib. Syst.
Security Symp., 2001, pp. 35–46.

[14] Y. Chen, I. Lin, C. Lei, and Y. Liao, "Broadcast authentication in
sensor networks using compressed bloom filters," in Proc. 4th
IEEE Int. Conf. Distrib. Comput. Sensor Syst., 2008, pp. 99–111.