ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

Sec-DiDrip: A Distributed Data Dissemination Protocol with Enhanced Security

Sruthi K1, Binoy DM Panicker2

M Tech Scholar, Department of CSE, LBS College of Engineering, Kasaragod, India[1]

Assistant Professor, Department of CSE, LBS College of Engineering, Kasaragod, India[2]

Abstract: A Wireless sensor network (WSN) is a network together with sensor nodes that connected through wireless media. After the deployment of a WSN some common variables such as sensing interval, data sending interval or small programs stored in each node of the network may need to be updated or changed. Since sensor nodes are distributed in ad hoc fashion manual updating is not always possible. So we use data dissemination protocols to alter the sensor configuration parameters. Two main drawbacks are suffered by existing data discovery and dissemination protocols. First, they are based on the centralized approach; in this approach only base station can disseminate data items. Such an approach suffers from single point of failure. Second, most protocols assume that working environment is safe, so attackers can easily harm network. In Wireless Sensor Network, the security and confidentiality of data is very important. This paper proposes a secure and distributed data dissemination protocol named Sec-DiDrip. It allows multiple authorized network users to directly disseminate data items to the sensor nodes. Sec-Drip enhances ensures the confidentiality of disseminated data hence enhances security.

Keywords: Wireless Sensor Network; Security; Data Dissemination; Confidentiality: Data Encryption.

I. INTRODUCTION

Wireless Sensor Network consisting of a number of sensor nodes that are connected through wireless media. It is used for a number of applications such as environmental monitoring, battlefield surveillance, and homeland security domains, national defense, national security, environmental monitoring, traffic management, health care, manufacturing, anti-terrorism and other disaster areas. Wireless sensor networks have become a growing area of research and development and are characterized by severely constrained computational and energy resources, and an ad hoc operational environment. These networks are currently receiving significant attention due to their unlimited potential. After the deployment of wireless sensor network (WSN), there is usually a need to update old small programs or parameters stored in the sensor nodes. Application requirements may change due to evolving conditions so network behavior need to be changed by introducing new code or updates. As manual updating is impossible the new code to the sensor nodes need to be propagated through air. This process of reprogramming a WSN is known as dissemination. This can be achieved by data dissemination protocol. This protocols can be used by the source to inject small programs or parameters to sensor nodes. There are many popular dissemination protocols available for wireless sensor networks. Classical protocols like Drip, Dip and DHV have a problem of been not secured. So malicious users can disseminate faulty data to the network with these protocols. This can be prevented using secure dissemination protocols. Almost all the data dissemination protocols are centralized in nature i.e. they consider a single base station which disseminates data or code into the sensor network [2]. This approach suffers from the single point of failure as dissemination is not possible when base station fails. Centralized method is inefficient and non-scalable. In a distributed approach authorized users can disseminate data items simultaneously into the WSN without relying on the base station. The eavesdropping attack is a serious problem in wireless sensor network (WSN). As the name implies it means listening to messages or data packets in transit through the wireless medium. It is a prerequisite for many other kinds of attacks. There are two types of eavesdropping attacks in WSNs [8].

Program images or code updates disseminated through the wireless medium can be grabbed by adversaries using this attack. To prevent disclosure of information through this attack the messages must be secured using some encipherement techniques like symmetric or asymmetric encryption. Security in wireless sensor networks is important for monitoring applications in military and civilian operations. For such applications updating the program image securely is more important. For example, in environmental monitoring applications unauthorized users should not gain any idea about the transmitted program image. It is essential that we provide authenticity, confidentiality and data freshness for the data dissemination. The confidentiality of this data dissemination cannot be compromised at any cost [9].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

Rest of this paper is organized as follows. In section two a survey on existing distributed dissemination protocol is given. Section three describes the proposed Sec-DiDrip in detail. Section four presents the advantages of Sec-DiDrip over basic DiDrip. Finally section five concludes this paper.

II. RELATED WORKS

The paper [1] proposed by Daojing He et al, is a code dissemination protocol suitable for a distributed environment. In this protocol multiple network users are allowed to disseminate data items to sensor node without depending on base station. This distributed code dissemination protocol includes a network owner, network users and sensor nodes. After the registration network users can disseminate data. Network owners are actual signers whereas the users are proxy signers. A cryptographic technique called proxy signature by warrant is used This dissemination protocol is denial of service attack resistant. The paper [2] proposed by Daojing He et al. is a secure and distributed code dissemination protocol named SDRP. In this protocol different users have different privileges. Privileges are assigned by the network owner. It uses a technique called identity-based cryptography. For secure distributed data dissemination Certificate Based Approach (CBA) is followed. Each user will have a public-private-key pair. User signs the code image using ECDSA algorithm before dissemination. DIDRIP [3] proposed by Daojing He, Sammy Chan, Mohsen Guizani and Haomiao Yang is a secure and distributed data dissemination protocol. DIDRIP comprises a network owner, users and sensor nodes. Network owner has a public-private key pair. Each network user gets a certificate after registering with the network owner. Users also have a public private key pair and dissemination privilege. When user needs to disseminate data he will construct the packet and signs with his private key. User certificate is also transmitted along with acknowledgement packet. This certificate is used by the nodes for authentication. There are some efficiency problems with this DIDRIP. It is not efficient in communication since the certificate need to be transmitted with the advertisement packet. Also signature verification is expensive because certificate should always be authenticated first. Some protocols ensure Authenticity and Integrity. Confidentiality of data is an important aspect but it is not ensured by any existing distributed data dissemination protocol.

III. PROPOSED WORK

A. Sec-DiDrip

Each node in the WSN should receive a copy of disseminated data. For this the Trickle algorithm [5] is used, which is used by most dissemination protocols. In order to ensure the freshness of data version number is used. Each data item is identified by the tuple (key, version, data).Since sensor nodes are resource limited devices a light weight block cipher encryption algorithm is used for encrypting the disseminated data. The algorithm used is based on chaotic maps and genetic operations which is suitable for wireless environment. The proposed Sec-DiDrip consists of four phases, system initialization, user registration, packet creation and packet verification. In system initialization phase, the network owner creates its public and private keys and encryption key, and then loads the public parameters on each node before the network deployment. In the user registration phase, a user registers with the network owner to get dissemination privilege. In packet creation phase, if a registered user wants to disseminate some data items, he/she will need to construct the data dissemination packets, encrypt the packet and then send them to the nodes. In the packet verification phase, a node verifies each received packet. If verification pass, it updates the data according to the received packet. In the following, each phase is described in detail.

1. System Initialization

At the initialization stage the base station runs an ECC to derive private key X and corresponding private key y. After that the related public parameters are preloaded in each node of the network. An encryption key is also established by the base station. For encryption key establishment an elliptic curve over prime field is used. This key along with User id and privilege level of each user is pre loaded in each node.

2. Registration phase

In the user registration phase user with the identity UIDj, needs to register with the bases station in order to obtain privilege level. User requests for the privilege level by submitting 3-tuple <UIDj, Prij, PKj> to the network owner, where Prij is the privilege level of user UIDj. PKj is the public key of the user. User UIDj chooses the private key SKj from GF field over q and computes the public key PKj= SKj*Q. After receiving the request the network owner uses ecdsa to sign the tuple with its private key. This tuple is send to each sensor node.

3. Packet Creation Phase

After completing the registration phase a user can disseminates data items to nodes. Suppose that a user say UIDJ wants to disseminate n data items: di = {keyi; versioni; datai}, i = 1,2, . . . , n. User first needs to encrypt the data items using the lightweight encryption algorithm. The algorithm proposed in [10] is used for encryption. For that a Pseudo random bit sequence is to be generated initially. This sequence is used in encryption process and is generated using

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

chaotic functions. Merkle hash tree [6] method is used for the construction of data packet. Merkle hash tree is constructed as follows. Initially all the data items are treated as the leaves of the tree. The hash value of two child nodes is computed and concatenated to form each internal node. This process is continued until the root node Hroot is formed, resulting in a Merkle hash tree. After the construction of tree the root of the tree is signed by the user UIDj using his private key SKj. Then transmits the advertisement packet P0 comprising user id UIDj, Hroot and SIG_SKj (Hroot). Subsequently, user UIDj disseminates each data item along with the appropriate internal nodes for verification purpose.

4. Packet Verification Phase

When a sensor node, say Sj, receives a packet either from an authorized user or from its one-hop neighbours, it first checks the packet's key field. If this is an advertisement packet P0= {UIDj; rootj; SIG_SKj{root}}, node Sj uses the UIDj to pick up the dissemination privilege Prij. Then examine the legality of Prij. If the result is positive, node Sj uses the public key y of the network owner to run an ECDSA verify operation to authenticate the signature. If yes, node Sj stores <UIDj; root> included in the advertisement packet; otherwise, node Sj simply discards the packet.

Otherwise, it is a data packet Pi, where i = 1, 2, . . . ,n. Node Sj executes the following procedure:
Node Sj checks the authenticity and integrity of Pi through the already verified root node received in the same round. If the result is positive and the version number is new, node Sj then decrypt the data (decryption algorithm is same as encryption algorithm), updates the data identified by the key stored in Pi, otherwise, Pi is discarded.

IV. DISCUSSION

The main objective of Sec-DiDrip is to solve the efficiency problems in DiDrip and enhances the security of DiDrip by ensuring confidentiality of disseminated data. There are lot of communication overhead due to the generation, transmission and verification of certificate in the basic protocol. In DiDrip first, the user registers with the network owner and gets a certificate. Then, when the user needs to disseminate data, first he has to send the advertisement packet before the data packet. The previously generated certificate is send along with the advertisement packet. So it is not efficient in communication because in sensor node this per-message overhead result in more energy consumption. Second, nodes run expensive verification algorithm to authenticate the certificate. The above two problems are solved in Sec-DiDrip. For that, in the initialization phase the public key and privilege level of each user is pre loaded in each node. When a new user is joined his id (UID) and public key are sent to each node by the network owner using his private key. When user disseminate data to the sensor node, first he sends the advertisement packet along with the user id (rather than certificate) and the root of Merkle tree signed with his private key. In order to authenticate a user, node picks up privilege level from its storage to check its legality. Then authenticate the signature using ecdsa verify operation. As with the basic protocol Sec-DiDrip ensures authenticity and integrity. Additionally confidentiality of data items is ensured by encrypting the data items using a light weight encryption algorithm. Thus only authorised nodes are able to decrypt the confidential information. Thus security is enhanced.

V. CONCLUSION

Security is the need of the hour in data dissemination. In WSN as attackers can send bogus data into the network to cause false updates or denial of service attacks. Also due to the open nature of wireless channels, messages can be easily intercepted. So secure protocol that ensues confidentiality, integrity, authenticity and freshness of data is must for data dissemination. Sec-Didrip is a secure and distributed data dissemination protocol that can be used for the secure and efficient dissemination of data in wireless sensor networks.

REFERENCES

[1]. Daojing He, Chun Chen, Sammy Chan and Jiajun Bu, "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transaction on Wireless communication, VOL. 11, NO.5, MAY 2012.S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[2]. Daojing He, Chun Chen, Sammy Chan and Jiajun Bu, SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 59, NO. 11, NOVEMBER 2012.
[3]. Daojing He, Member, IEEE, Sammy Chan, Member, IEEE, Mohsen Guizani, Fellow, IEEE, Haomiao Yang, Member, IEEE, and Boyang Zhou "Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks".
[4]. Daojing He, Sammy Chan, Mohsen Guizani, "Small Data Dissemination for Wireless Sensor Networks: The security Aspect" IEEE. 2014
[5]. P. Levis et al, "Trickle: A Self-Regulating Algorithm for Code Maintenance and Propagation in Wireless Sensor Networks", Proc. NSDI, 2004.
[6]. R. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE Security Privacy, 1980, pp. 122–134.
[7]. Jisha Mary Jose, "Security Issues During Data Dissemination in Wireless Sensor Networks", International Journal of Advanced Research Trends in Engineering and Technology, March 2015.
[8]. Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi WingWong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas" ,International Journal of Distributed Sensor Networks Volume 2013.
[9]. Zi Feng, Jianxia Ning, Broustis, Pelechrinis, K. Krishnamurthy, Faloutsos, Michalis, 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks.
[10]. Kamanashis Biswas, Vallipuram Muthukkumarasamy, Kalvinder Singh, An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks, ARTICLE in IEEE SENSORS JOURNAL· DECEMBER 2014.