ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Distributed and Secure DiDrip Protocol for Data Discovery and Dissemination in WSNs

Savitri[1], Sheela Sridhar[2]

P.G. Student, Department of Computer Science & Engineering, BNMIT, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Computer Science & Engineering, BNMIT, Bengaluru, Karnataka, India[1]

ABSTRACT: In the wireless sensor networks (WSNs) a data discovery and dissemination protocol is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes. Previousdata discovery and dissemination protocols suffer from two drawbacks such as, they are based on the centralized approach; i.e, only the base station can distribute data it 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. Hence to overcome from those drawbacks DiDrip protocol is used, which is the secure and distributed data discovery and dissemination protocol, It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Moreover, as demonstrated by the theoretical analysis, it addresses a number of possible security vulnerabilities that have identified. Extensive security analysis show DiDrip is provably secure and also implement DiDrip in an experimental network of resource-limited sensor nodes to show its high efficiency in practice.

KEYWORDS:Distributed Data Discovery, Security, wireless Sensor Networks, Efficiency.

I. INTRODUCTION

There is necessary to amend buggy/outdated small programs or parameters stored in the sensor nodes thereafter a wireless sensor network is deployed. Data discovery and dissemination protocol is used to achieve updating in the sensor nodes, which alleviates a source to inject abrupt programs, queries, commands and configuration parameters to sensor nodes. Note that it is distinctive from the code dissemination protocols such as data dissemination or reprogramming protocols, where it disburses large binaries to reprogram the each sensor in the network.

For example, a binary file of tens of kilobytes necessitates a code dissemination protocol for efficacious dissemination even though disseminating sundry two-byte configuration parameters obligates data discovery and dissemination protocol. In consideration of the sensor nodes could be scattered in a harsh environment, remote approach for disseminating such succinct data to the sensor nodes by way of the wireless channel is a more accustomed and empirical approach compare to manual intervention.

In concede of liberal studies, there are manifold data discovery and dissemination protocols for WSNs. DHV, DIP and Drip are esteemed as the state-of-the-art protocols amidst those adduced protocols and have been encompassed in the TinyOS distributions. All proffered protocols postulate that the WSN is trustworthy and has no adversary for operating environment. However, in reality, adversaries exist and impose threats to the normal operation of WSNs. This issue has only been addressed, which identifies the security vulnerabilities of Drip and proposes an effective solution.

More importantly, all existing data discovery and dissemination protocols employ the centralized approach in which 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

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.
The networks of our concern have multiple owners and multiple users. The users of the network get the authentication certificate by requesting the network owner. The network owner provides different users with different dissemination privileges.

II. SYSTEM REQUIREMENTS

To be utilized productively, all PC programming needs certain equipment segments or other programming assets to be available on a PC. These essentials are known as (PC) framework necessities and are frequently utilized as a rule instead of a flat out standard. Most programming characterizes two arrangements of framework prerequisites: least and prescribed. With expanding interest for higher handling force and assets in more up to date variants of programming, framework prerequisites tend to increment after some time. Industry examiners recommend that this pattern have greater impact in driving moves up to existing PC frameworks than innovative progressions.

- **SOFTWARE REQUIREMENTS**
  - Operating system : Linux (Ubuntu)
  - Software : Network Simulator 2.35
  - Programming languages : Tool Command Language, AWK, C++
- **HARDWARE REQUIREMENTS**
  - Main processor : Dual Core
  - Hard disk capacity : 80GB
  - Cache memory : 2 GB

III. IMPLIMENTATION DETAILS

DiDrip Protocol mainly includes five phases to disseminate the data between the nodes among the wireless sensor network. Figure 1 shows the system architecture for DiDrip Secure protocol, which shows the data discovery and dissemination of data from source to destination through the authorized users only. where it contains the following mechanisms:

- Network Owners
- Authorized users
- Sensor nodes

Advantages
- Proposed approach is suitable for multi-owner-multi-user WSNs.
- Identified the security vulnerabilities in data discovery and dissemination when used in WSNs.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

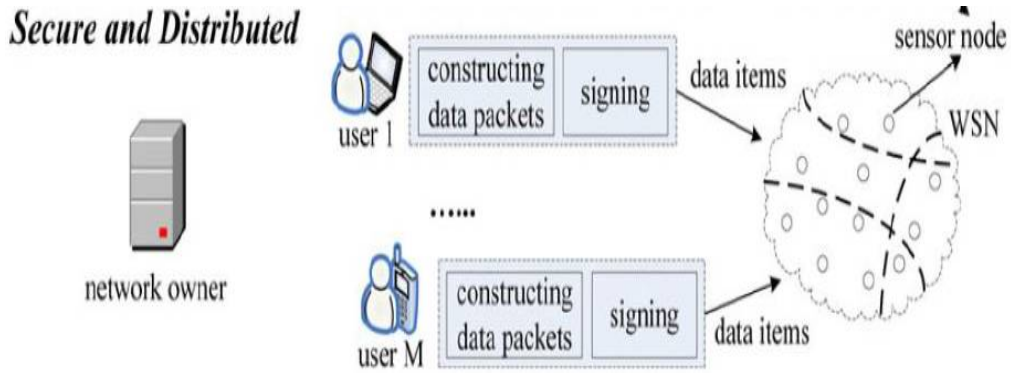

Fig 1 : System Architecture of DiDrip

The protocol consists of four phases namely, system initialization phase, user joining phase, packet preprocessing phase and packet verification phase each of which are described in detail in the following sub -sections. The Table 1 shows the notations that are used in the description. The flow of information processing at network owner, network user and sensor nodes is shown in Fig. 2.

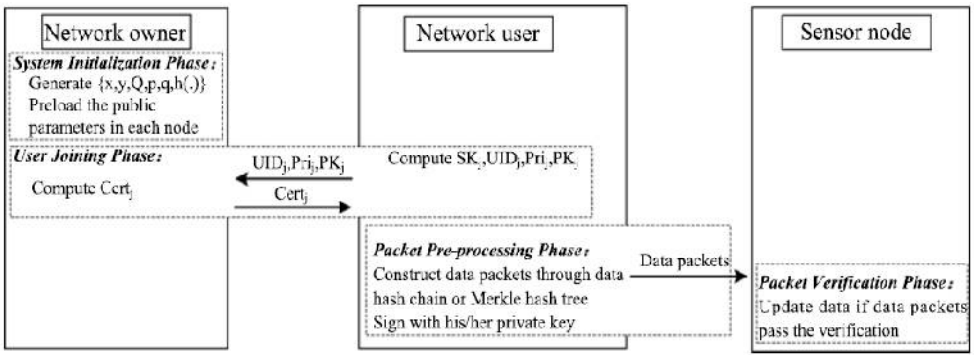

Fig 2 : Information processing Flow in DiDrip

NOTATIONS

Notation	Description
UID_j	Identity of user U_j
PKj	Public key of user U_j
SK_j	Private key of U_j
Pri_j	Dissemination privilege for user U_j
$Cert_j$	Certificate of user U_j
$SIG_k(M)$	Signature on message M with key k
h(M)	Hash value of message M
|| or ,	Concatenation of two bit streams

TABLE 1 : Notations

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A. ***System Initialization Phase***

160 bit Elliptic curve cryptography is set up in this phase. The network owner performs the following steps.

- Choose two big prime numbers p and q each of 160 bits long.
- Select an elliptic curve E over GF(p)
- Select private key x ϵ GF(q).
- Compute the public key y = xQ where Q is the base point of E and is of 320 bits long. y is 160 bits long.
- Load the public parameters {y, Q, p, q} in each node.

B. User Joining Phase

When any user, say Uj wants to join the network and obtain the dissemination privileges, the user joining phase is invoked. The user requests for the certificate from the network owner. The steps are as follows.

- Consider a network user U_j with the identity UID_j which is of two bytes.
- User chooses a private key $SK_j \epsilon GF(q)$
- User computes the public key $PK_j = SK_j.Q$
- User sends a 3-tuple $< UID_j, Pri_j, PK_j >$ to the network owner.
- The network owner generates the certificate and sends back to the user U_j.

$Cert_j = \{ UID_j, PK_j Pri_j, SIG_x\{h(UID_j \| PK \| Pri_j)\}\}$

Since user ID is of two bytes, 65,536 users can be supported. The length of privileges field is of 6 bytes andhence the certificate generated is 88 bytes long.

C. Packet Pre-processing Phase

When a user enters the network and has some information to disseminate over the network, first it has to construct the packet. This is done in packet pre-processing phase. The following steps are performed.

- The user constructs the packet by using Merkle hash tree method.
- Here a tree is constructed taking n data items.
- The data items act as the leaves of the tree.
- At the upper level, internal nodes are constructed by concatenating two child nodes.
- Continue constructing the nodes until the root node is formed. It is labelled as H_{root}.
- Thus obtained tree is the Merkle hash tree with depth $D = \log_n(n)$.
- The user, before dissemination of actual data items,
  - Signs the root node $H_{root}$with SK_j.
  - Sends an advertisement packet P0

  $P0 = \{Cert_j \| H_{root} \| SK_j(H_{root})\}$
- After sending P0, the user disseminates further packets along with the appropriate internal nodes. In Merkle hash tree method, each packet contains the D hash values.

D. Packet Verification Phase

When any sensor node receives the disseminated data, it has to first verify whether it is from authorised user, whether that sensor node ID is included in the node identity set of Pri_j and whether the packet maintains data integrity. The following steps are performed.

- If the packet received is advertisement packet

  $P0 = \{Cert_j \| H_{root} \| SK_j(H_{root})\}$, check for the privileges.
- If the result is positive, then check for the authenticity if certificate by using the public key, y of the network owner.
- If certificate is valid, check for the validity of signature.
- If the result is positive then store $<UID_j, root>$, otherwise discard the packet.
- If the packet received is a data packet other than P0, the sensor node checks for the authenticity and integrity.
- For positive result, it checks for the freshness of the data. If the packet received is a newer version, then it updates its data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

IV. EXPERIMENTAL RESULTS

The network simulator tool NS2 version 2.35 is used to simulate the results. Initially a network is deployed with 15 nodes as shown in Fig.3. Nodes 11, 12, 13 are considered to be the network owner and these authorises the network users by providing the certificates to them as shown in Fig.4 which is user joining phase. Once the users obtain the dissemination privileges via the certificates, they start disseminating the data packets as shown in Fig.5. The Fig.6 shows the execution time of the hash function for various input bit streams of variable length.

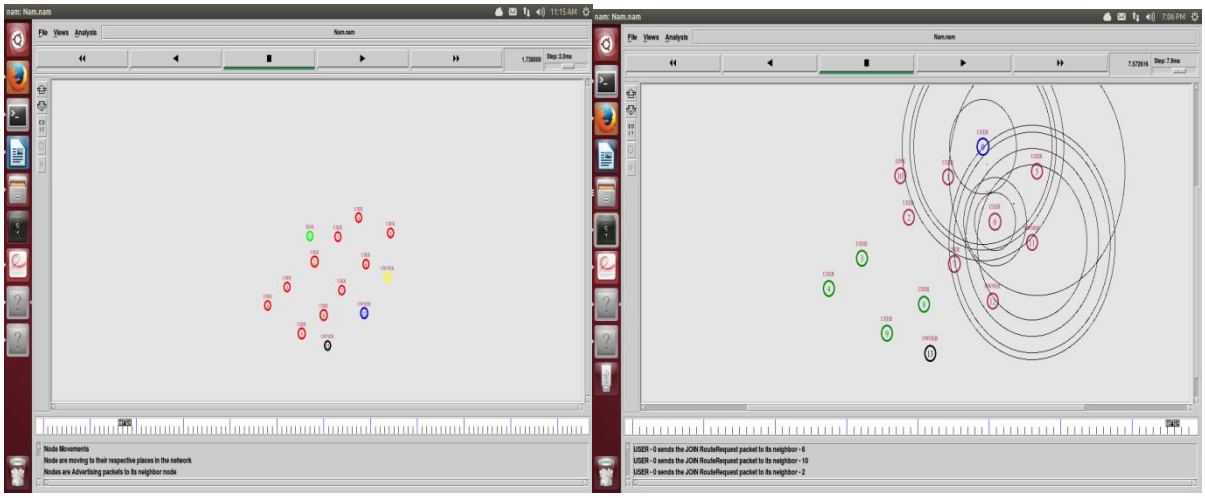

Fig 3 : Setting up of Network Fig 4 : User Joining phase

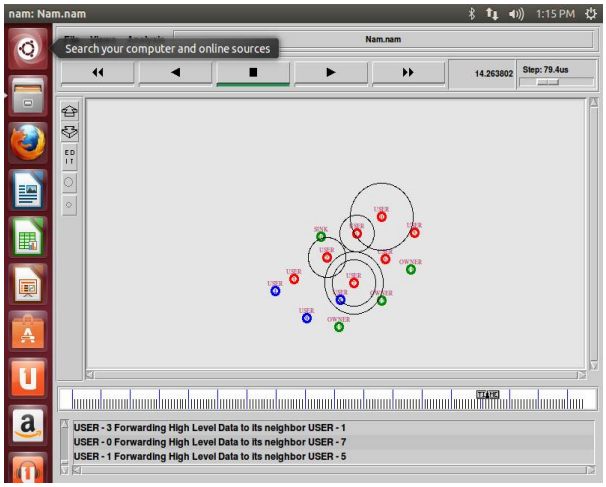

Fig 5 : Broadcasting of Data Packets

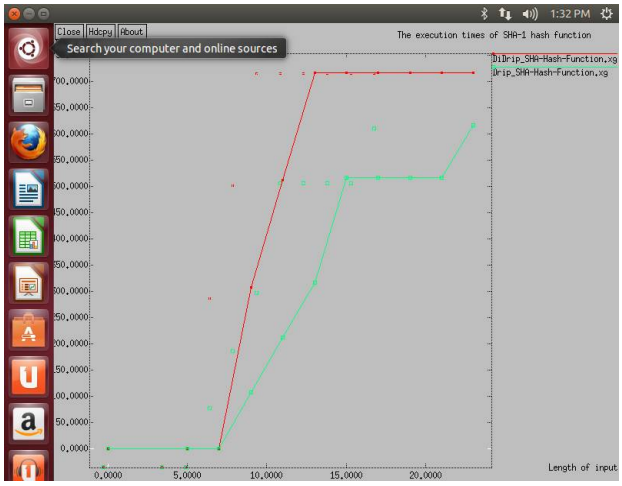

Fig 6 : Propagation delay comparison

V. CONCLUSION AND FUTURE WORK

This paper proposes a secure and distributed protocol for data dissemination in wireless sensor networks. This addresses the drawbacks associated with centralized approach of data dissemination. Also the security vulnerabilities

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

which were the major issues to be concerned in earlier approaches are addressed here. This paper provides data authentication by a secure hash function along with Merkle Hash Tre e method for digital signature. Data integrity is provided using Elliptic Curve Cryptography which is a strong encryption technique. As a future enhancement, additional security measures like data confidentiality can be added and efforts can be made to reduce the memory and energy overheads.

REFERENCES

[1] D. He, S. Chan, M. Guizani and H. Yang, "*Secure and distributed data discovery and dissemination in wireless sensor networks*", IEEE Transaction on Parallel and Distributed Systems, pp. 1045-9219, 2013.
[2] 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, Sept. 2013.
[3] 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.
[4] S. Rahman, N. Nasser, T. Taleb, "*Secure timing synchronization for heterogeneous sensor network using pairing over elliptic curve*", Wireless Communications and Mobile Computing, vol. 10, no. 5, pp. 662-671,May 2010.
[5] T. Dang, N. Bulusu, W. Feng and S. Park, "*DHV: A code consistency maintenance protocol for multi –hopwireless sensor networks*", in Proc. EWSN, pp. 327-342, 2009.
[6] M. Ceriotti et al., "*Monitoring heritage buildings with wireless sensor networks: The Torre Aquiladeployment*", in Proc. IEEE IPSN, pp. 277-288, 2009.
[7] Sangwon Hyun, PengNing, An Liu, Wenliang Du, "*Seluge: Secure and DoS-Resistant Code Disseminationin Wireless Sensor Networks*", IEEE computer society, 978-0-7695-3157-1/08, 2008.
[8] K. Lin and P. Levis, "*Data Discovery and Dissemination with DIP*", in Proc. ACM/IEEE IPSN, pp. 433-444, 2008.
[9] G. Tolle and D. Culler, "*Design of an application-cooperative management system for wireless sensornetworks*", in Proc. EWSN, pp. 121- 132, 2005.
[10] J.W. Hui and D. Culler, "*The dynamic behavior of a data dissemination protocol for network programmingat scale*", in Proc. ACM SenSys, pp. 81-94, 2004.