Enhanced and Secure Distributed Data Discovery and Dissemination in Wireless Sensor Networks

1Shivkant Rai, 2Prof.Shailendra Gupta, 3Prof.Pankaj Richhariya
Department of Computer science and engineering
Bhopal Institute of Technology and Sciences
Shivrai11@gmail.com
shailuonline@gmail.com
Hodcs.bitsbhopal@gmail.com

***Abstract*— Now a day's Wireless sensor networks (WSNs) are the most popular technique so that Protocols such as the data dissemination and data discovery is going to be completely responsible for scattering commands to management as well as it updates the parameters used in configuration to the participating sensor nodes. Two major drawbacks encountered in the previous protocols that are used for dissemination and data discovery that they follow the approach which is centralized in manner; that means firstly the data can be distributed by the base stations only. In multi-owner-multi-user scenario of wireless networks this type of old approach is not good. Secondly very less security is used when these protocols were designed so that it was very easy to made attacks on such kind of unsecure scenario to destroy the network. Hence to overcome this we proposed a new technique here named as E-DiDrip, which is safer and efficient than the older ones. In this approach number of privileges are assigned to multiple users present in network which are authorize by network owners so that users can easily distribute the data items in the network of sensor nodes.**

***Keywords*— Wireless sensor networks, efficiency, distributed data discovery and dissemination, security.**

I. Introduction

In Wireless sensor network (WSN), when we use this we have a lot of tiny old programs on which this network works or we can say that damaged or bugged programs too so that we have to eventually change or more precisely replace that and also gradually updates the various parameters stored in the nodes of the sensor network. We have a lot of ways to do that but we prefer a more precise method or say protocol to do this, so that in which by using very small small queries are inserted into the sensor nodes and this source of medium is delivered by the data discovery and dissemination protocol. As if now we leave the old and non-efficient protocol of data dissemination which reprograms the very complex network using large binaries. As for the better explanation if we took the example of dissemination the large amount of binary files say in KB's then this will require the dissemination of the code using protocols, whereas the above said protocols are compulsorily required in such configuration parameters used in disseminating several 2-bytes. As we making a focused approach so that this method of distributing the data in such a small amount in the various sensor nodes remotely is more impactive or practical rather than the manual intervention.

1.1 Wireless Networks

As we all know that in this electronic and modern era of technology now a day's wireless networks is more preferred rather than the traditionally wired system so that we can able to archive high bandwidth in this wireless networks too and by this we can also conclude that this type of network is the best method or medium to transport the data between the modern devices equipments or the traditional wired system.

As we all know that this wireless network works on bandwidth or say coverage of various range so that we can easily be categorize into three popular categories (a) wireless wide area network in this category we have a wide area of range to cover so that we uses Global Communication System or cellular (2G or 3G) in which we can obtain wide area of coverage for better results. (b) In this second type of category we uses Ethernet, HyperLan and other LAN technologies which are wireless in nature for good communication. (c) In this third type of wireless communication mechanism we have wireless personal area network (WPAN) which includes the infrared technology and Bluetooth as well.

All these are tetherless that means we are not using any kind of wire for communication or say that all are done by electromagnetic waves. Various wavelengths having various frequency bands extend upto 9 kHz and we have also limitless radio frequencies so that we will move into infrared spectrum frequencies and beyond that we can enter into the visual spectrum.

1.2 Wireless LANs

We have more flexibility or we can say grater portability while using the wireless local area network so that in this we are not really connected by the old or traditionally wired system in which we are completely depend on the single wired connection; WLAN provides the wireless adaptors so that each device is equipped with this to make the wireless connections and provide us more flexible and convenient way to connect with the network. These adaptors are the connected using RJ-45 jack or port with the wired LAN.

As described above devices are mounted with various access points and all the devices thus communicated using those access points which will cover area upto 300 feets and increasing as technology increases, Range or cell is the technical word used for that coverage area.

These access point can merged with each other in result we found better network coverage. Wireless LANs are the most popular way of network communication now a day by using this we can frequently connect with the network very easily.

1.3 Ad Hoc Networks

The network which is used to connect with the remove devices in a dynamic manner such as Bluetooth is known as Ad-hoc network. As the nature of the shifting topologies, we name it as “as-hoc” network, as we previously discussed that the wireless LANs have rigid infrastructure whereas the ad-hoc network easily maintain the random configuration characteristics of network. In this kind of network we have a master/slave scenario by using this various wireless devices are connected and communicated with each other.

In this master/slave scenario the master is going to control the data flow and changing topologies say in the piconet of the Bluetooth formed. Each time the network will have to reconfigure so that meets the need of continuously changing wireless devices and thus we have a bunch of routing protocols to do so.

1.4 Wireless Sensor Network

Wireless sensor networks are the most advanced form so that it is used to monitor or store the critical environmental parameters such as pressure, temperature and sound frequencies etc. in which this we are able to transmit or record the data very easily while there is a huge change in the readings and able to pass or forward the result within the network. As we already know that most of the modern networks are bi-directional in nature and this whole concept of wireless sensor network is motivated by military applications, so the in their advanced stage they are often used in various customer based applications also such as health monitoring, process monitoring etc.

As the name indicate that a wireless sensor networks are made of one node or many nodes that are mutually connected to each other. Radio transceiver with antenna, electronic circuit to interface sensor, microcontroller and the energy source such as battery are the core parts of a wireless sensor node.

As there is no limit of technology hence the size of the sensor nodes can also be possibly ranging from various sizes accordingly but also cost effective accordingly to the use, so that this will be the biggest barrier to use and become common to all about this technology and all are connected hence other limitations such as bandwidth, memory and computational speed are also accounted as the limitations. As it we talk about the topology as it would again varies from the range of various basic to advanced topologies.

1.4.2 Wireless Devices

The various ranges of the devices use the wireless technologies, use of handheld devices being the most prevalent form today. The most commonly used wireless handheld operative devices are the smart phones, PDA's and text messaging devices

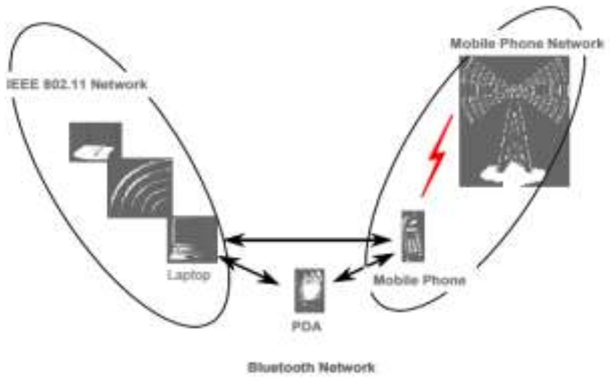


Figure.1 National AD Hoc Network

II. LITERATURE SURVEY

In here this literature survey, the multiple data discovery and the dissemination security protocols [7], [9], [10], [6] now have been used for the Wireless Sensor Networks. Drip [10], DIP [9], and DHV [6], are being used for the security purpose in the Wireless Sensor Networks. This is the main issue that has only going to address recently by which it identifies security issues of the Drip protocol and thus proposes an efficient and effective solution. The centralized approach is inefficient, non-scalable and vulnerable to the security attacks that can be merely launched from any- where along with the communication path [10]. Although even worse, when some of the Wireless Sensor Networks does not have base stations at all. Existing research thus depends on location of its information and it is not always obtained very easily, accurately [1] and efficiently. In terms of networks the Multicast communication is now becoming basis of growing number of user's applications. Therefore, in securing the multicast communication is the most important strategic requirement for the effective deployment for large scale business in the multi party applications [1]. The main issues in securing the multicast communication are the sources authentication services.

1. DRIP

Sensor Network Management System (SNMS) [10] is mainly designed to be most simple and to have minimal impact on the memory and the network traffic, while the remaining is open and flexible. The core system is now evaluated in light of the issues that are derived from the real deployment experiences. Wireless sensor networks act as in the aggregate, and hence, a SNMS must be able to arrange and manage in the aggregate. The aggregate management thus requires a dissemination protocol which can deliver the messages very reliably to a set of network nodes within a sensor network. The algorithm is used by our dissemination layer is Trickle algorithm.

Trickle [2] algorithm uses periodic retransmissions to ensure the eventual delivery of the message to every sensor node in the network. To reduce the number of required messages, the retransmissions can now be suppressed by the prior transmissions of the similar messages, and the randomization is going too used to prevent the permanent suppression. [10] Dissemination layer now takes the Trickle retransmission algorithm and thus builds the transport-layer interface. In SNMS the dissemination protocol, named as Drip, now provides the transport layer interface to the multiple channels of reliable message dissemination.

2. DIP

A dissemination protocol known as DIP is a data discovery and dissemination protocol for wireless networks [9]. In the Prior approaches, such as [3] SPIN or trickle, we have overheads that can scale linearly with number of the data items. Suppose for the T items, protocol DIP can be identify the new items with the O (log (T)) packets while maintaining an O (1) detection of latency.

DIP protocol is a hybrid approach for data detection and dissemination. In this, it separated into two parts: detecting that the difference occurs, and also identifying which of the data item is the different. Here DIP dynamically used a combination of scanning and searching based on the network and the version of the metadata conditions [9]. In its decisions, the DIP continually estimates the real probability that in this a data item is different. The DIP maintains these important estimates through the message exchanges. Now when the probabilities reach to 100%, the DIP is exchanges the actual data items. Here it is an eventual consistency Protocol in which, when data items are not frequently changing, all of the nodes will be eventually looks like a consistent set of data items.

3 DHV

This protocol is a code consistency maintenance protocol (Vertical search, Horizontal search and Difference detection). This protocol focuses as the main objective to overcome the disadvantages of the previous protocols like DIP [9] and DRIP [10] by overcome or we can say that reducing complexity. In this the data items are going to be represented as tuples (key, version).If in here the two versions are different; they might be only difference in a few least significant bits of the version number rather than in the all of their bits.

The protocol DHV [6] includes the two important phases: first Detection phase and the second is Identification phase. In the detection phase, each node will have broadcast the hash of all its compatible versions in form of SUMMARY message .Unlikely in the identification phase, the vertical and the horizontal search steps are used. In the horizontal search, node broadcasts the checksum of all the versions, called a HSUM message. In the vertical search, node is going to broadcasts a bit slice, which is starting at the least significant bit of all the versions, called a VBIT message. Now, after identifying this, node is going to broadcasts those (key, version) tuples in a VECTOR message.

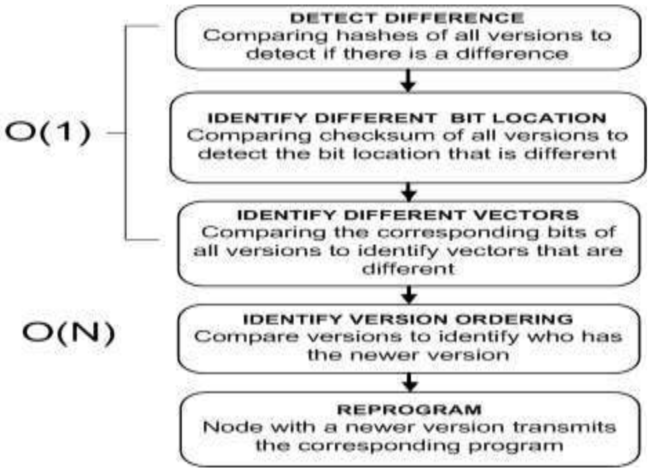

O(1)
O(N)
DETECT DIFFERENCE
Comparing hashes of all versions to detect if there is a difference
IDENTIFY DIFFERENT BIT LOCATION
Comparing checksum of all versions to detect the bit location that is different
IDENTIFY DIFFERENT VECTORS
Comparing the corresponding bits of all versions to identify vectors that are different
IDENTIFY VERSION ORDERING
Compare versions to identify who has the newer version
REPROGRAM
Node with a newer version transmits the corresponding program

Figure 2: Main steps in the DHV protocol

III. PROBLEM FORMULATION

In the existing system we found that there are more chances to get attacks on the network that concludes the security is less. Whenever the connection between node and base station is broken, data discovery and the dissemination are impossible.

IV. PROPOSED SOLUTION

In here the proposed solution as the DiDrip Protocol is mainly includes the five important phases to disseminate data between the sensor nodes among the wireless sensor network. The Figure 2 shows system architecture for the DiDrip Secure protocol, which now shows data discovery and the dissemination of the data from the source to the destination through only authorized users. Where it having the following mechanisms:

- Sensor nodes
- Authorized users
- Network Owner

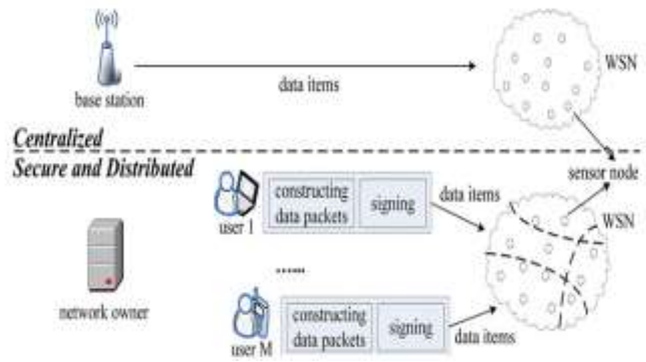


Figure 2: DiDrip System Architecture

The proposed protocol is consisting of four phases, the system initialization phase, the user joining phase, the packet pre processing phase and the packet verification phase, each of the following are described in detail below in sub - sections. Table 1 shows notations that are going t be used in the description. The flow of the information processing at the sensor nodes, network user and network owner, is shown in Figure 2.

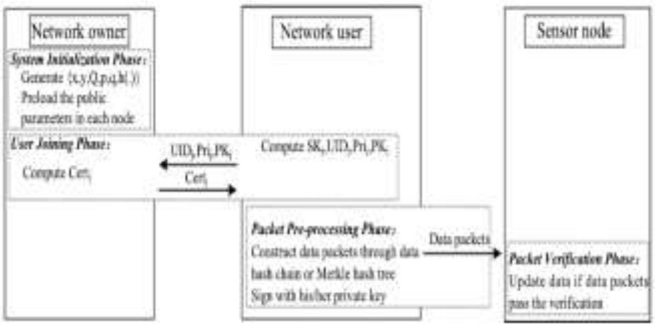
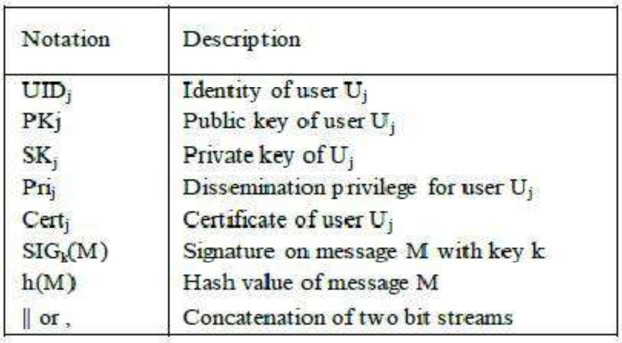

Network owner
System Initialization Phase:
Generate {x,y,Q,p,q,h(.)}
Preload the public parameters in each node
User Joining Phase:
Compute Cert$_j$
UID$_j$,Pri$_j$,PK$_j$
Cert$_j$
Network user
Compute SK$_j$,UID$_j$,Pri$_j$,PK$_j$
Packet Pre-processing Phase:
Construct data packets through data hash chain or Merkle hash tree
Sign with his/her private key
Data packets
Sensor node
Packet Verification Phase:
Update data if data packets pass the verification

Figure 2: DiDrip Information processing flow



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

A. System Initialization Phase

In this phase, 160 bit Elliptic curve cryptography is set up and network owner going to perform the following steps.

- First choose the two big prime numbers p and q each of which is 160 bits long.
- Select an elliptic curve E over GF(p)
- Select the private key x ϵ GF(q).
- Now Compute the public key y = xQ where Q is the base point of E and 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 there any user, say Uj going to join network and going obtain dissemination privileges, then the user joining phase is invoked. User thus requests for certificate from the network owner. The dedicated steps are as follows.

- First consider a network user Uj with identity UIDj which is of only two bytes.
- The user chooses the private key SKj ϵ GF(q)
- The user computes a public key PKj = SKj.Q
- Now user sends the 3-tuple < UIDj, Prij, PKj> to network owner.
- Network owner now generates the unique certificate and sends it back to the user Uj.

Certj= { UIDj,PKjPrij, SIGx{h(UIDj || PK || Prij)}}

Since the user ID is of in two bytes, 65,536 users can be now supported by this. Length of the privileges field is of the 6 bytes and thus the certificate generated is 88 bytes long.

C. Packet Pre-processing Phase

Whenever a user enters in the network and he has some sort f information to disseminate over sensor network, it has to be constructing the packet first and this is be done in the packet pre-processing phase. Rest following steps are performed as follows:

- User first constructs the packet by using the Merkle hash tree method.
- In this a tree is to be constructed taking n number of data items.
- Now the data items act as leaves of that tree.
- In the upper level, the internal nodes are thus constructed by concatenating the two child nodes.
- Now continue constructing sensor nodes until root node is going to be formed. It is now labelled as Hroot.
- Now, the obtained tree is Merkle hash tree with the depth of D = log n(n).
- The dedicated user, now before the dissemination of the actual data items,
    - Signs the root node Hroot with SKj.
    - Sends the advertisement packet P0
      P0 = {Certj || Hroot|| SKj(Hroot)}
- After sending P0, User disseminates the further packets along with appropriate internal sense nodes. In this Merkle hash tree method, each and every packet contains the D hash values.

D. Packet Verification Phase

Whenever their any of the sensor node receives disseminated data, it immediately going to first verifies whether it is from the authorised user or whether that the sensor node ID is included in node identity set of Pri_j , whether the generated packet maintains the data integrity. Here are the following steps which are performed.

- In this, if packet received is an advertisement packet P0 = {Certj || Hroot|| SKj(Hroot)}, then check for the privileges assigned.
- If result is completely positive, then we check for authenticity and if the certificate is created using the public key, y of the network owner.
- Now, if the certificate is fully valid, then check for validity of the signature.
- If result is hopefully positive then we are going to store <UIDj, root>, otherwise we discard the packet.
- Again, if the packet which we received is a data packet other than the P0, then the sensor node first checks for the authenticity and the integrity.
- Now, for the positive result, it definitely checks for freshness of the data and if the packet received is a newer version of that, it is going to updates its data.

V. CONCLUSION

In this paper we proposed the most secure and distributed protocol for the data dissemination in the wireless sensor networks. This will going to addresses the core drawbacks that are associated with the centralized approach of the data dissemination. Also in this the securities vulnerabilities which were the most major issues are to be concerned in the earlier approaches and are addressed here. IN this paper we provided the data authentication mechanism by the most secure hash function along with the Merkle Hash Tree advanced method for the digital signature. The data integrity is provided by using the Elliptic Curve Cryptography method, which is the one of the strongest encryption technique. As in the future enhancement, the additional security measures like the data confidentiality can surely be added and the efforts can be made to reduce memory and the energy overheads.

REFERENCES

[1] 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" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[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] 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.

[9] K. Lin and P. Levis, "*Data Discovery and Dissemination with DIP*", in Proc. ACM/IEEE IPSN, pp. 433-444, 2008.

[10] G. Tolle and D. Culler, "*Design of an application-cooperative management system for wireless sensornetworks*", in Proc. EWSN, pp. 121- 132,2005.

[11] 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. In Proc 2nd Int. Conf. Embedded Netw. Sensor Syst., 2004, pp. 81–94

[12] NildoRibeiro Junior, Marcos A. M. Vieira, Luiz F. M. Vieira, and Om prakash 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.