ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

WSN with Secure Data Discovery and Dissemination

[1] Deepali Ausekar , [2] Prof.Trupti Agarkar
[1] [2] Department of Electronics and Communication
[1] [2] Ramrao Adik Institute of Technology, Nerul Navi Mumbai, India

***Abstract*—Wireless Sensor Networks (WSNs) contains large number of sensor nodes where sensor nodes are used to sense environmental parameters e.g. temperature, humidity etc. It senses data, process and transmit it and sometimes there is need to disseminate data through wireless links to adjust configuration parameters of sensors or distribute management commands and quires to sensors. Several Data dissemination protocols have been proposed to address this need but all follow Centralized Method.**

In this paper we have proposed DiDrip protocol to disseminate Data items which follows distributive approach to make WSN more efficient and secure.

***Keywords*—WSN,Data dissemination,DiDrip.**

I . INTRODUCTION

A wireless sensor network (WSN) which is consists of distributed sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. After the deployment of Wireless sensor network (WSN) buggy old small programs or parameters stored in the sensor nodes should be updated usually. The data discovery and dissemination protocol is used to update these programs and parameters which facilities a source to inject small programs, commands, queries and configuration parameters to sensor nodes. In this paper Secure Distributive approach is proposed using DiDrip.

In this following section i.e. section II is Literature Survey which consists of information about nature of existing protocols with their drawbacks and some security issues regarding WSN data dissemination. Section III consists of description of Design features and Needs. Section IV is description of basic DiDrip in detail. Section V Describes actual performance according to simulation and finally section VI is overall conclusion.

II. LITERATURE SURVEY

Some data discovery and Dissemination protocols has been invented e.g. Drip [4] [2] ,DIP [5], and DHV [3]. DIP is used to detect different data item .This is modification in trickle but both follows centralized method which is not secure. Trickle, Drip gives information about health of nodes. DHV reduces difficulties of the DIP and Trickle as it uses tuple (key, version, and data) to represent data items it also detects differences in data items but it is better than that of DIP protocol as it reduces the transmitted bytes but here DoS attacks may happen and again it uses centralized scheme. In Drip Standard message reception interface is provided. But all of these Drip, Trickle, DIP, DHP does not provide security and uses centralized approach or communication.

Most important thing is that all of the above data discovery and dissemination protocols [6] does not provide security at the best level and all these all protocol uses centralized scheme as [7] shown in fig. 2 i.e. only base station can disseminate data item and big disadvantage of this method is that if the base station is not working whole networks stop to operate. If base station and node are disconnected then dissemination is not possible. It is not useful when there are WSNs without base station and so it become inefficient .E.g. If we are using WSN to monitor illicit crop cultivation, it can be attacked by other party as base station is attractive target so there is need of distributed data dissemination under authorized network user.

III. DIDRIP

DiDrip is best extension of all existing protocols. Its key feature is that it is used for privileging number of network users by giving them different priorities to some specific dissemination operation. DiDrip includes four steps of operation in WSN followed by Initialization of basic, User registration, Packet construction and Packet Verification. In initialization network owner creates private and public key. In second step user comes into network having separate user ID and priority level to do certain task given by network owner. In third step Packets are constructed

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 4, April 2017

followed by some specific pattern like 3-tuple and are sent to the nodes. Packets are nothing but data items which are sent by user to node. These data items are always in encrypted format. In packet verification step each data item is verified by checking its key field. If result of operation is rue then data is updated otherwise it will be rejected.

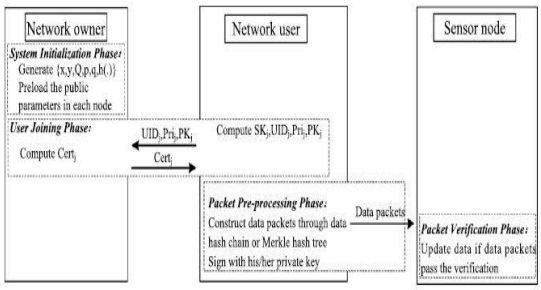

Fig. 1 Basic DiDrip performance [16]

Initialization of basic system

- At first ECC is run by network owner establishing elliptic curve over prime field.
- Private key x is created by network owner.
- Some basic parameters (y, Q, p ,q, h()) which are public are then created and loaded in each sensor node of the network
- Public key is created by using x as y = xQ

where Q is basic point of curve E ,P is large prime number and E is over GF(p).is also large prime number and it is order of Q.awe have considered 160 bit ECC. Here y and Q both are of 320 bits whereas p, q are of 120 bits

User Registration

This step is accessed by network user when it wants its privilege level

- Network owner Uj sends 3-uple (UIDj, Privj, PKj) to the network user where UIDj is the user identity, Privj is the privilege level for dissemination and PKj is public key derived by user.
- Public key PKj = SKjQ
- Network owner receives this 3-tuple of user
- It will then create certificate for network user i.e.Certj = (UIDj, PKj, Prij, SIG) Here size of UIDj is of 16 bits.It means there are 65536 network users. Size of PKj is 320 bits and that of SKj is 160 bits. SIGx is discripted as signature on message that is in bracket with key x. Privj is of 6 bytes.

Packet construction

In this step packets of data items are constructed by using Merkle hash tree [15] or data hash chain method. Merkle hash tree creates more overhead than that of data hash chain. Actually in Data hash chain only one hash value is used for packet as in case of Merkle hash tree number of hashes are equal to tree depth and there is no need of packet sequence like data chain method.

- In this user comes into WSN
- It sends di = (key i, version i, data i), wherei = 1,2,…,n.
- By using any method i.e. data hash chain or Merkle hash tree packet is constructed.
- In Data hash chain packet p consist of packet header and hash value of next packet.
- Hash value of next packet is used to verify next packet.
- Merkle hash tree is constructed in second method.

Packet Verification

Whatever data item/packets constructed in last step are received by sensor nodes.

- Sensor node receives packet.
- It then make more attention o the privilege Privj in the received packet.
- It checks authorization of privilege to decide whether that packet is intended to it or not.

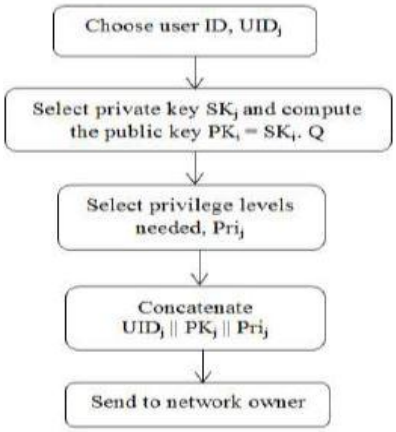

Fig 2. Steps Performed by network user

ISSN (Online) : 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 4, Issue 4, April 2017

- If result of above is true sensor node will take use of public key y to run ECDSA.
- It will run ECDSA to verify certificate.
- If verification output is positive then signature is authenticated and packet is verified otherwise it is discarded

Sensor node also verify the integration as well as authentication of data item means all data is covered in packet r not and is it sent by authorized user depending on status of version. It will accept the packet for new version. It updates data accordingly otherwise it just discards data packet

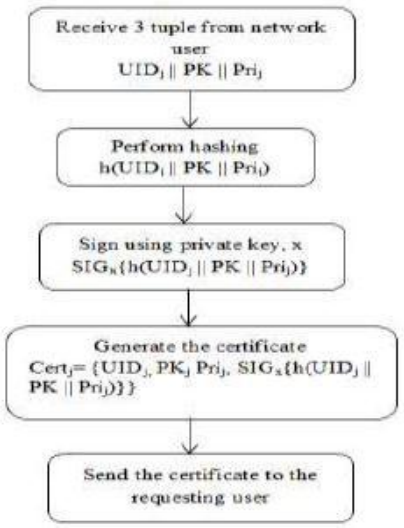

Fig 3. Steps Performed by Network Owner [14]

IV PERFORMANCE ANALYSIS

fig 4. shows Graph of Energy consumed by Network, Network Energy is nothing but node energy As number of node Increases Computation power increases so Overall network energy varies with respect to number of nodes as shown

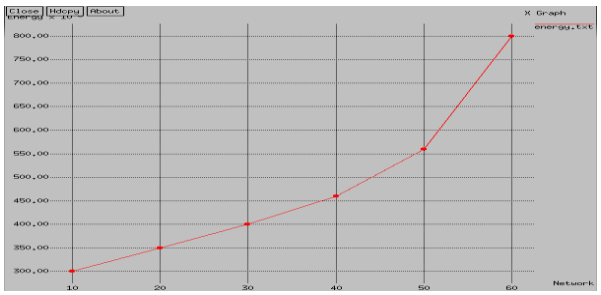

Fig. 4 Overall Energy Consumed by Network

V CONCLUSION

In this paper we have used DiDrip protocol for secure data discovery and dissemination in network of resource limited sensor nodes. We have eliminated centralized method of distributing of data by only base station by giving different privileges to different users. Security is also provided without consumption of much energy by sensor nodes. Two main disadvantages of existing systems are avoided first is, instead of centralized base station approach we have used multi-owner and multi-user concept, second is we have provided authorization according to privilege.

VI FUTURE WORK

In existing system Certificate is created by network owner which is transmitted to all network users to provide privileges but in this process of creation and transmission overhead increases which again consumes energy. It can be eliminated by sending only pair of (public key, user Privilege) to each sensor node so that overall duty cycle can be minimized to make WSN more energy efficient.

REFERENCES

[1] J. W. Hui and D. Culler, The dynamic behavior of a data dissemination protocol for network programming at scale, in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst.,2004, pp. 8194..

[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. 19461956, May 2012.

[3] 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. 327342.

[4] 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. 121132.

[5] K. Lin and P. Levis, Data discovery and dissemination with DIP, in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw., 2008, pp. 433444.

[6] 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. 277288.

[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] M. Rahman, N. Nasser, and T. Taleb, Pairing-based secure timing synchronization for heterogeneous sensor networks, in Proc. IEEE Global Telecommun. Conf., 2008, pp. 15.

[9] P. Levis, N. Patel, D. Culler, and S. Shenker, Trickle: A self-regulating algorithm for code maintenance and propagation in wireless sensor networks, in Proc. 1st Conf. Symp. Netw. Syst. Design Implementation, 2004, pp. 1528.

[10] 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. 3546.

[11] 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. 99111.

[12] R. Merkle, Protocols for public key cryptosystems, in Proc. IEEE Security Privacy,1980, pp. 122134. 23

[13] M. Bellare and P. Rogaway, Collision-resistant hashing: Towards making UOWHFs practical, in Proc. Adv. Cryptology, 1997, pp. 5673.

[14] http://www.google.co.in/basic wsn

[15] A. Perrig, R. Canetti, J. Tygar, and D. Song, Efficient authentication and signing of multicast streams over lossy channels, in Proc. IEEE Security Privacy, 2000, pp. 5673.

[16] 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" 24