ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Data Propagation and Renovation of Nodes in Wireless Sensor Networks

B.Kiranmai
Student,
Dept of IT,
SNIST, Telangana, India.

G.Sumalatha
Assistant Professor,
Dept of IT,
SNIST, Telangana, India.

ABSTRACT:

Wireless sensor networks are basically distributed networks or a collection of sensor nodes which collect information which are used to analyse physical properties or environmental conditions. In everyday life we occur via sensor networks which give the weather condition details in our smart phones and many such applications. Most of them require regular updating of software in sensor nodes through the wireless channel for efficient management and working. A good data dissemination protocol must be secure, reliable and energy efficient and less complex.

All the existing protocols suffer from the centralized approach and are not accurate. Here we introduce a new protocol DiDrip i.e. Data discovery and Dissemination in Routing Information Protocol , which is on cryptographic technique which prevent the traffic and all the network attacks such as Dos, man in the middle ,pollution attack, with this we can securely transfer the data to the nodes and update the sensors which are not working properly. This protocol provides total security, authenticity, integrity and confidentiality of the data which is disseminated on each sensor node and even in every communication.

Keywords:
Dissemination, DiDrip, authenticity, integrity, Confidentiality.

I.INTRODUCTION:

Wireless sensor network (WSN)[2] are used for information gathering on large scale data rich environments.

Every sensor node is usually need to update the old small programs, commands or parameters stored in it. This can be achieved by the data discovery and dissemination protocol, which ease a source to inject or update small programs, commands, queries and configuration parameters to sensor nodes when they are not working properly. In Wireless Sensor Network, the security of data and confidentiality of data is an important aspect. Hence the data cannot be interrupted by the intruder. Also we identify the security vulnerabilities and liabilities in all the existing data discovery and dissemination of nodes. The main function of this protocol is to give permissions to multiple network users. So, with the help of different security parameters the system provides a very high security to the wireless sensor network. Energy efficient new algorithm is also used because it is difficult to crack.

Section II Discusses about the Literature survey, Section III Discuss the Proposed Approach , Section IV Gives the Implementation and Results, Section V Gives the Conclusion and Future work, Section VI show the Reference papers.

II. LITERATURE SURVEY:

A data discovery and dissemination protocol, for wireless sensor networks (WSNs) is for updating configuration parameters and distributing management instructions and updating the old programs in the sensor nodes. Traditional protocols available for this include Drip, DIP and DHV all are based on security and authentication. They are all based on Trickle algorithm [6].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Drip proposed by Tolle et. al [7] is the mild of all dissemination protocols and is based on [6]Trickle algorithm and authorize an independent trickle algorithm for each variable in the data with some drawbacks. Every time an application wants to transmit a message or the data, a new version number is generated or created and then used. This cause the protocol to reset the Trickle timer and thus disseminate the new values else the trickle timer interval is added. DIP (DIssemination Protocol) [8] is a data detection and dissemination protocol proposed by Lin et al. It works in two parts: determining whether there is differences in the data stored at every node, and then determine which data is different or unique and compares with all the systems.

It is based on the concept of version number and key for each data item. DIP calculates hashes that cover all version numbers of the data. Nodes that receive hashed data which is same as their own know that they have consistent data with respect to their nearest neighbours. If a node gets a hash that differs from its own hash, it knows that a difference exists in the data. Fang Hong ping et.al [4] have classified Data Dissemination strategies into major categories based on basis of operation Push-based strategy, On-demand (or pull-based) strategy, hybrid strategy and data allocation over multiple broadcast channels.

A. Push Based Strategy:

Sensor data is pushed by all source nodes to the sink nodes through multi hop routing system. The queries resulted from sink nodes is retrieved without any communication cost. Its advantage is that it is efficient as it reduces push- query routing cost to zero. The disadvantages are (a) Communication cost in storage phase is comparatively high (b) Due to multi-hop routing, the neighbor nodes of sink nodes will undertake more data delivery task than any other sensor nodes, resulting in multiple hotspots, the system robustness and stability cannot be ensured.

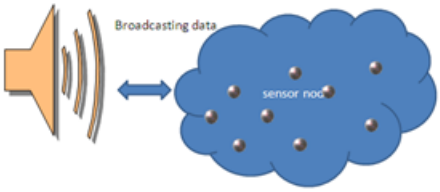

Fig 1: Data Broadcasting

B. Pull Based Strategy:

The pull-based Strategy adopts completely opposite idea to push-based Strategy. The source nodes stores data at home and wait for query passively. On the contrary, the consumer nodes broadcast all the query demands to source nodes all over the network on their own initiatives. Communication cost is less but the disadvantage is that some source nodes even if they have no, related data they have to participate in data delivery.

C. Push Pull (Hybrid) Strategy:

A better approach, called hybrid broadcast, combines push-based and pull-based techniques. This offer the combination between both the consumer node and source node.

III.PROPOSED SYSTEM:

In this proposed protocol the data dissemination is done in a secure and fast way by using the techniques of cryptography algorithms with a simulation tool such as NS2 all in one. DiDrip protocol updates the sensor nodes and reduces the number of retransmissions of packets due to any packet losses happening in the network by combining and sending data. Also data disseminated is always sent as encrypted data. For this nodes first perform node to node authentication and establish the session keys. The session keys are used for hashing the encrypted message and transfer of data packets. This protocol ensures that the system is free of pollution attacks [3] and Denial-of-Service attacks. The different phases of DiDrip are:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A. INITIALIZATION PHASE:

In this phase, an ECC algorithm is used for all cryptographic functions. The network owner will do the following steps to generate a private key x and some public parameters $\{y, Q, p, q, h(.)\}$. We select an elliptic curve E over $GF(p)$, where p is a very big prime number. Here Q denoted as the base point of E while q is also a very big prime number and denotes the order of Q. It then selects the private key $x \epsilon GF(q)$ and computes the public key $y = xQ$.then we will load all the public parameters to each node in the network.

B. USER JOINING PHASE:

In this phase the users say U_m who want to dissipate data to the sensor nodes can enter into the network. First the user with the user id UID_m wants to communicate with the sensor node, he should get the privileges from the network owner. The user U_m chooses a private key $SK_m \in GF(q)$ and computes the public key $PK_m = SK_j . Q$. The user will generate a 3-tuple id $<SK_m, PK_m, UID_m>$ and sends to the network owner. All these are encrypted with ECC and sent. Upon receiving the message the owner will generate the $Cert_m$ and also dissipation privileges Pri_m.The certificate consist of

$$Cert_m = \{UID_m, PK_m, Pri_m, SIG_x\{h(UID_m \| PK_m \| Pri_m)\}\}$$

C.PACKET GENERATION PHASE:

In packet generation phase the user say U_m will create a packet and enters into the wireless sensor network and dissipate n data items to the sensor nodes, the data $d_m = \{key_i, version_i, data_i\}$ where $i = 1,2,..n$. For constructing the data packet we use data hash chain method. The data hash chain method a packet say P_i is the packet header, d_i is the data and the hash value of packet P_{i+1} is generated to verify the next packet. The cryptographic hash H_i is calculated over the total packet P_i , not only the data portion d_i we establishing a chain of hashes. The user U_m uses his private key to run ECDSA sign operation to sign the hash value of the data packet $h(P_1)$ and then creates the advertisement packet P_0 i.e. $(P_0 = \{Cert_m, h(P_1), SIG_{SKm}\{h(P_1)\}\})$.

Similarly the network owner assigns a predefined key to identify the advertisement packet by the sensor node.

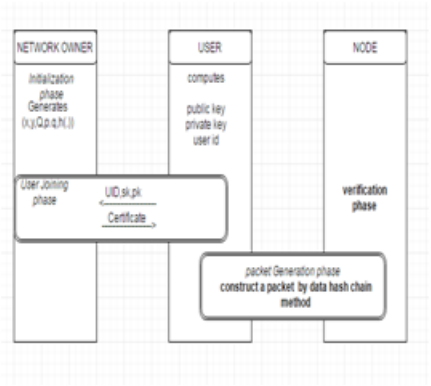

Fig 2: Phases in DiDrip

D. PACKET VERIFICATION PHASE

Now the function of sensor node comes, the sensor node say S_m , receives a packet from the authorized user of from the neighbour of the sensor node, it first checks the packet key field. The advertisement packet

$$(P_0 = \{Cert_m, h(P_1), SIG_{SKm}\{h(P_1)\}\})$$

The node S_m first check the legality of the dissipated privilege Pri_m .If the result is positive , node S_m uses its public key y of the network owner to run the ECDSA verify operation to check the hash function to authenticate the certificate. If the $Cert_m$ is valid, node S_m authenticates the signature. If everything is good node S_m stores $<UID_m, H_1>$ and this is included in the advertising packet. Otherwise the sensor node simply discards all the packets.

IV. IMPLEMENTATION AND RESULTS:

This protocol has been implemented in NS2. We have considered a network topology consisting of 100 nodes or more then 100 nodes and 25 different data variables are disseminated. We can implement this protocol in Linux operation system and also in windows. In windows by installing VMware software. In NS2 tool the results are accurate and the time complexity of this protocol is less then compared to other protocols. We have used ECC i.e. elliptical curve cryptography for encryption and decryption and also we have use SHA

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

and ECDSA algorithms [11] for hashing and signing the data packets to provide the confidentiality of the data. We use session keys for providing confidentiality. First the communication starts with the network owner and the network user who wants to disseminate the data. The user generates a 3-tuple message with encrypted form sends to the owner. The owner then decrypts the message checks the privileges and then he sends a certificate to the user, upon receiving the certificate the user then generates the packet that he want to update the nodes. All the data transfer between the owner and user, user and sensor nodes are very confidential. This new protocol is found to resist cases of pollution attacks i.e. only valid data packets are received and processed by the intermediate nodes in the network.

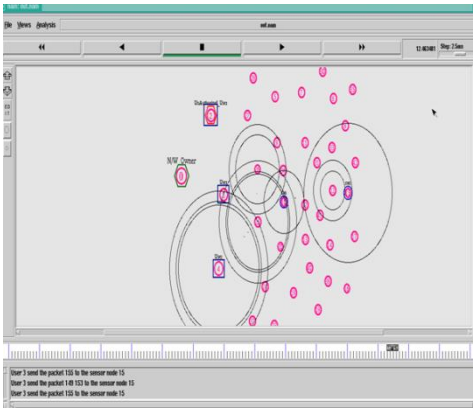

Fig 3: NAM Model

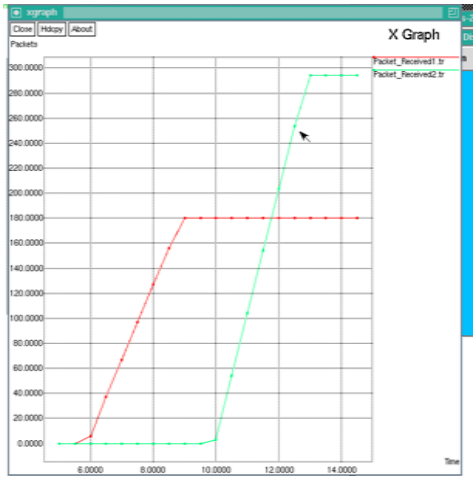

Fig 3.1: Packet Delivery Ratio

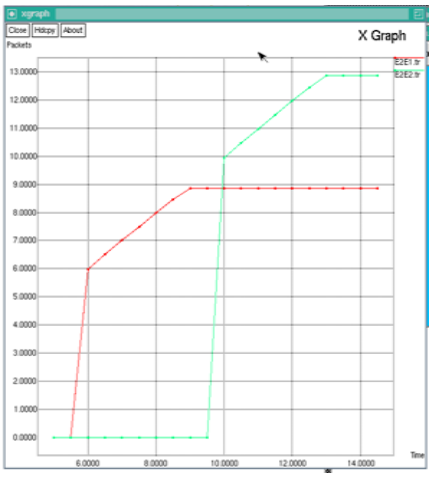

Fig 3.2: End to End delay

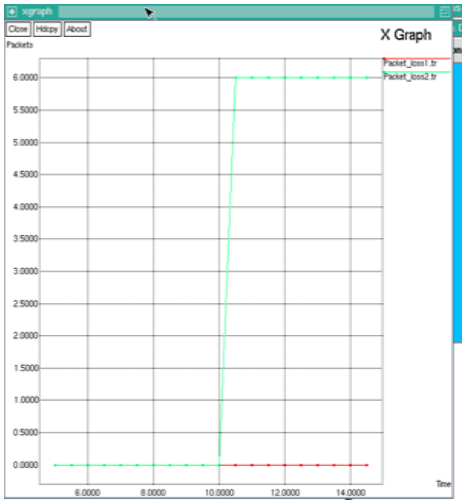

Fig 3.3: Packet Loss

V.CONCLUSIONS AND FUTUREWORK:

We have given a novel data discovery and dissemination protocol for wireless sensor networks which can be used to achieve secure and fast data dissemination especially for small configuration parameters and variables. This technique combines the concepts of network coding and simple cryptographic techniques so as to disseminate data. The advantages of this protocol are that it is resistant to pollution attacks, and achieves immediate authentication and confidentiality of data been disseminated. Session keys are used to encrypt the hash and send data between nodes. The disadvantage of this system is it has more time complexity because of SHA algorithm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In future work we can generate an algorithm which is easy and have less time complexity when compared to other hashing techniques.

VI.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]Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo, Li Xie, "Pollution Attack: A New Attack Against Localization in Wireless Sensor Networks", IEEE, WCNC-2009.

[4]I-Hong Hou, Yu-En Tsai, T.F. Abdelzaher, and I. Gupta. Adapcode: Adaptive network coding for code updates in wireless sensor networks. In INFOCOM 2008.The 27th Conference on Computer Communications. IEEE, pages 1517–1525, 2008.

[5]Daojing He, Sammy Chan, Shaohua Tang and Mohsen Guizani, "Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks", IEEE transactions on wireless communications, Vol. 12, No. 9, September 2013.

[6]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. 2004 NSDI, pp. 15-28.

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

[8]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.

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

[10] Hui, J.W., Culler, D.: "The dynamic behavior of a data dissemination protocol for network programming at scale, New York, NY, USA, ACM (2004) 81-94.

[11]Aqeel Khalique, Kuldip Singh "Implementation of Elliptic Curve Digital Signature Algorithm Volume 2 – No.2, May 2010.