A Study on Secure Data Collection Mechanism for Wireless Sensor Networks

Manivannan.P[1], Manivannan.D[2]
School of Computing, SASTRA University
Tirumalaisamudram, Thanjavur, Tamilnadu, India.
[1] mani.vannan238@gmail.com
[2] dmv@cse.sastra.edu

Abstract

Wireless sensor network is a collection of sensor that deployed to monitor physical and environment condition such as temperature, pressure, sound etc. In wireless sensor node event detect and passes the information to the base station, when the sensor nodes pass the information to base station and intruder may get the data easily from the sensor nodes. so objectives of this paper is to review various existing method to secure data collection mechanism.

I. Introduction

Wireless sensor network is a collection of sensor node with limited resources and base station. Sensor node monitors the physical and environmental condition such as temperature, sound, pressure, vehicular motion, humidity etc.. The network consists of a large number of sensor network and smaller number of cluster head and base station. Compared to the energy of cluster head is higher than sensor node energy .As a result event occurs when the sensor nodes sense the information passes through the base station so increase secure data collection. There are many security issues in wireless sensor networks namely predetermined path and node compromise etc. When sensor nodes sent the data using predetermined path attacker can easily get the data. other issues of WSN to compromise the sensor node and modify the data to pass the information through the base station. These problems solved by improving the sufficient and secure data transmission.

The rest of the paper is organized as follows: Section II Discuss as the detailed description of the various secure data collection mechanism .In Section III Compares various secure data collection method parameters. Finally paper concludes the study on section IV.

II. Overview of secure data collection methods

To ensure the reliability of the data transmission in wireless sensor networks various secure data collection methods have been proposed. In this section we are going to review some of those methods which have been developed in the recent year.

A. Secret Key information and collision resistant hash function

Secret key information and collision-resistant hash function proposed by Amar Rasheed, Ravi Mahapatra et al in [1].Mobile sink collect the data from the sensor node by the use of predetermined path.Using of predetermined path the intruder can easily modify the data .In proposing paper the efficient security scheme is used to secure the secret key information and collision resistant hash function use to authenticate the information to the base station. Mobility is based on two categories namely random and mobility control. Mobile node randomly collects the data from the sensor node and mobility control is fixed path to collect the data from the sensor node.

Secret Key establishing and Collision resistant hash values distribution schemes: mobile node sent the individual key to the sensor node for the encryption process. After the encryption process sensor node passes the information to the mobile node. The Mobile node sends the data to the base station for decryption. After decryption the mobile node sends the hash value information to the sensor node because intruder can’t sent the false hash value information to the network. So authentication purpose is used for collision-resistant hash function and another scheme based on efficient one-way hash chains.

B. Secure Data Collection

Secure data collection proposed by Yan Zhejiang al in [2].In Tiered wireless sensor network we propose secure data collection for the protest of data by using data confidentiality and data integrity. Master key based on end to end encryption and used in Data confidentiality (i.e.) sensor node should not leak the data to neighbor node because of sink node randomly select master key and shared the key to each node. Every round update shared key by using one way key techniques. In SDC protocol consist of two phases namely system setup, time based query and data verification.

System setup: System setup can easily detect the neighbor list and storage agent. We assume that each sensor node with one neighbor of individual id and storage agent. If more than one storage agent or individual id the sensor node chooses randomly to avoid collision. The Time based query and data verification is mainly used for authorized user only and the sink is mainly intermediate between user agent and storage agent.

C. Key pridistribution

Key pridistribution proposed by Durresi.A, Barolli.l al in [3]. Wireless sensor network is mainly used for military applications so we have to use key predistribution for separate key pools. The separate key pools to connect mobile sink to the stationary nodes to send data. Mobile nodes move dynamically to collect the data from stationary nodes. Key predistribution can secure the data between the mobile node and stationary node. Mobile node randomly selected the key pools to reduce the key compromised on the network and connect the stationary node by using the session key for security purpose.

D. AES-128 Encryption

AES-128 Encryption proposed by Huang Y.m, Heiegh m.y al in [4].Health net is mainly used for health monitoring and secure data collection from the network. Health net is nothing but body sensor network. Health net is used to communicate the mobile sensor node. Mobile sensor nodes are mainly used for storing the data and securely transfer the data from one device to another device. In hospital many patient are stored the data securely, so the data transfer securely to another parities(medical experts, relatives and his family).so we have to use confidentiality secure data collection by using zigbee AES-128 encryption between sensor node and hub.AES 128 encryption is mainly used for secure data transfer, When sensor node send the data and passes through the base station, unauthorized user easily get the data from the sensor node, so we have to used AES-128 encryption method. In AES-128 encryption is mainly used for authorized person only access the medical data. For examples To implement by using password method. If enter the welcome page user put the password. If it is authorized user can access the patient data. If unauthorized doesn’t open the data. When logout data, automatically erase the decrypt key from the system. Shared key is mainly used for authenticate purpose because connection between patient and medical expert, family.

E. N to 1 Multipath discovery protocol

N to 1 Multipath discovery protocol proposed by Wenjing Lou al in [5].In this paper hybrid multipath scheme is mainly used for security and reliable data collection from one source node to destination node. N to 1 multipath discovery protocol is mainly used to find the multiple node disjoint path from all sensor node to base station to 1 multiple discovery protocol main technique is hybrid data collection scheme. The multipath discovery protocol is two phase (I) branch aware flooding (ii) multipath extension of flooding. Branch aware flooding is used to ability of finding extra paths because limiting of nodes sent message between sensor node and neighbor nodes. Multipath extension of flooding is used to find the more node disjoint path of each sensor node at cost of some extra message exchange.

F. MGKE Group based key establishment

MGKE Group based key establishment proposed by al in [6].Sensor nodes are static and mobile nodes are moving to collect the data from the cluster head. When mobile node moving to collect the data from the cluster head and attacker can easily modify the data from the sensor node, after passes information to the base station. So propose this paper is MGKE group based key establishment scheme is used group based sensor deployment.MGKE is mainly used unique pair wise key to connect the neighbor nodes and security.MGKE is very carefully to set the key between sensor node and mobile node because if unauthorized identify the key and easily get the data from the individual sensor node .so, it avoid the every sensor node share the key with one another. Each sensor node sharing the key with one another and create a own group. So each sensor create one or more groups. Sensor node si shares the key with any other neighbor node sj but if si and sj are same group doesn’t share the key with each other. Each sensor node shared secret key with base station and mobile collector secure collect the data from the sensor node and pass the information to the base station.

G. Secure Fault-Tolerant data collection

Secure Fault-Tolerant data collection proposed by Jyh-ming Huang,shih chieh Tai al in [7] .CRINet is a secure and fault -tolerant data collection scheme is mainly used for group KEY management mechanism, reduce rekey operation and high reliability sensing data transferred to the base station .CRINet scheme main thing is split into several group and sensing field. Base station can be divided into sensing data and transmission power etc.. All sensor nodes are same groups and same group id.finally each group leader sends encrypt the group list id and pass the information to the base station. EBS (Exclusion basis system) is mainly used for group key management system and optimal key set parameters are i, j, k. I is number of rekey messages, j is used size of group is used number of key stored in every member of nodes.Group head update phase is mainly used avoid compromised node. If node is compromised, EBS will randomly create cluster head and passes EBS key set to such nodes and Every nodes sharing key with neighbor nodes, because it will avoid the unauthorized access the nodes.

H. Secure Group communication

Secure Group Communication proposed by Chung skewing al in[8].Secure group communication is mainly used for confidentiality, authenticity and securely message deliver to the base station. Secure group communication is mainly used to key graphs and group communication main advantage one or more authorized sender, authorized receiver and more efficient securely transmit the large groups. Securing unicast communication mainly based on client and server.intially client and server is authenticating because secure group communication used symmetric keys shared each other. If client wants join the group already client and server is used by authentication protocol. So SCP will easily accept the group and server key share the each group member is called individual keys. In group communication, servers transmit the key to all group members and maintain user –keys relation. For example :there are three subgroup, each group three member(n1,n2,n3)(n4,n5,n6)(n7,n8,n9)Each member will give three keys(i) individual key (ii) key for subgroup (iii)key for entire group because if one member leave means it can easily add another member and securely sharing the key transmitting to the data. Secure group is mainly depends on keys server because of securely transmit the key to the user-groups.key server mainly know that key set, user set and user-key relation. Every user is used individual key shared by key server because of confidential communication with the key server.

Rekeying strategies and protocol is mainly used for securely transmit data because if user should join the group, secure group request to the key server. Join group authenticate between user and server, if is authorized user it will join group suppose if it is not authorized and leave the group. There are three rekeying strategies user oriented, key-oriented,and group-oriented. User-oriented rekeying is mainly consider on each user create a new key and mainly consider on each new key encrypt individual key.

I. Time stamp protocol and Polynomial point sharing protocol

Time stamp protocol and polynomial point sharing protocol by proposed al in [9].Wireless sensor network is mainly concerate on increase network lifetime. Mobile data collectors collect the data from the cluster head to passes information through the base station. So main thing is securely and unauthorized easily get the data from the mobile data collector. So propose this paper time stamp protocol, polynomial point sharing protocol. Time stamp protocol is mainly used security’s it mobile data collection every round going to collect the data from the cluster head, finally pass information through the base station. if mobile data collector sent session key to cluster head and cluster head check it is original MDC request or malicious request. If it is original mdc request means cluster head encrypt the data and passes to the MDC.finally mdc pass the information through to the base station

Polynomial point sharing protocol is mainly used for securely and sharing key with two cluster head, if one cluster head sent the key to mobile data collector and another cluster head sent the key to mdc.if two cluster head key is equal then only mdc collect the data from the cluster head. If cluster head key is not equal mdc doesn’t get the data from the cluster head.

J.Randomized multipath delivery

Randomized multipath delivery proposed by Tao shu,sis Liu And marwan karuz al in [10].Data delivery mechanism main drawback is black hole attack. When using multipath routing attacker can easily get the data .so it avoid multipath routing.if randomly sent the data to the designation and attacker doesn’t get the data easiler.Sensor node sent the data sent randomly and can save more energy .so proposing paper the randomized multipath delivery is used sent the data securely by using multihop routing. Each node randomly select by neighbor nodes.

Purely random propagation is mainly based on one –hop neighbour.if sensor node sent the information from the source to designation and mainly based on neighbor list and all sensor node id.when sensor node sent the information to the sink node based on TTL values.

Direct random propagation is mainly based on increase efficiency by using two-hop neighbor information.

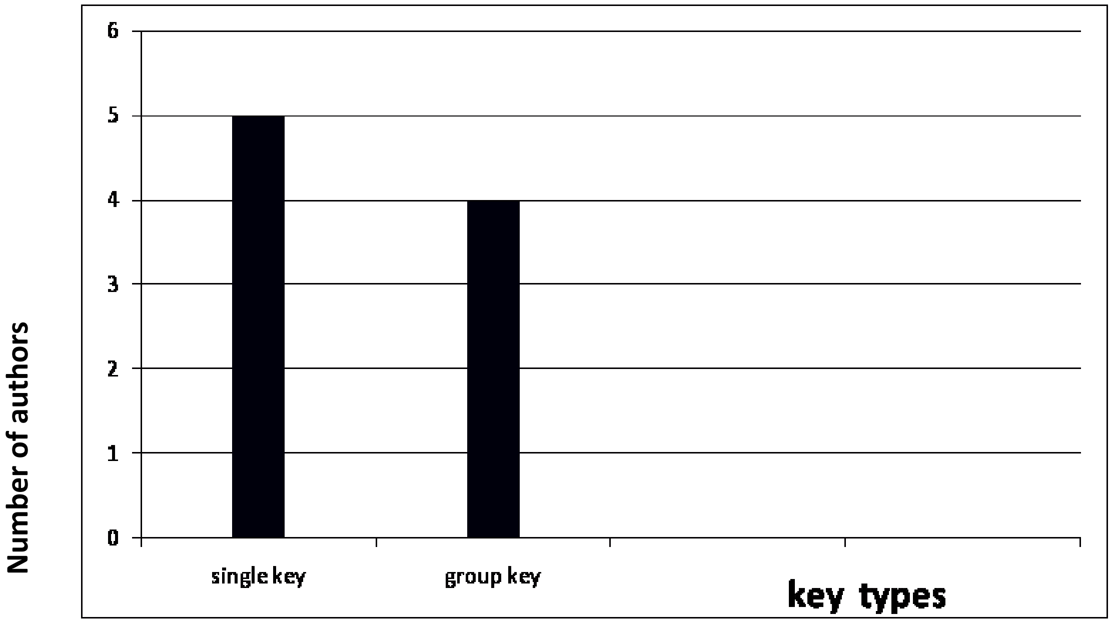
III. Comparison of Secure data collection

This paper collected various securely data collection method for wireless sensor network. In this section the comparison of various secure data collection methods.Tabel 1 shows the comparisons of various secure data collection methods discussed in the section II.Generally the secure data collection method have some common characteristic which are single key, group key and attacker/problem.

Author	Method	Security using single key	Security using Group key	Attacker/ Problem
Amar Rasheed,Ravimah epatra[1]	Secret key information and collision resistant hash function	Yes	No	Wormhole attack
Yan Zhao Zhejiang ein [2]	Secure data collection	No	Yes	Data Confidentiality attack, Data integrity Attack
Durresi,A Baroli,I [3]	Key Predistribution	Yes	No	Compromised Node
Haug Y.m,Heiegh m.y[4]	AES-128 Encryption	Yes	No	Compromised Node
Wenjing Lou [5]	N to 1 Multipath discovery protocol	Yes	No	Collision attack
Lizhou and Jinfeng Ni and Chinya V.ravikumar [6]	MGKE group based key establishment	No	Yes	Eavesdropping attack
Jyh-ming Huang,shih chien Tai [7]	Secure and Fault-Tolerant Data collection	No	Yes	Eavesdropping attacker
Chung Keiwong [8]	Secure group communication	No	Yes	Scalability problem
A.S Poornima ,B.B Amberker [9]	Time stamp protocol, Polynomial point sharing protocol	Yes	Yes	Wormhole attack
Taoshu,Sis Liu And marwan Karunz[10]	Randomized multipath delivery	Yes	No	Black hole attack

Table 1: Comparison of secure data collection methods

The following graph shows an analysis report of various secure data collection methods discussed in section II



IV. Conclusion

In this paper various secure data collection discussed in section II have been studied and comparisons of these methods were presented in table 1.In single key security mechanism, there may be change of unauthorized user can access the data if user gets the key. But In group key mechanishm, eventhrough user got some key, user can't access the data, because to access the data user need all the keys.so,group key security mechanism provides high security for data in wireless sensor network.

References

[1] Rasheed, a:mahapatra.r. "Secure data collection scheme in wireless sensor network with mobile sink", IEEE international symposium on network computing and applications, pages 332-340,2008.

[2] Yang zhao:zhiguang:youtao zhang, " Secure data Collection for time based queries in tiered wireless sensor network", 15th IEEE international conference on embedded and real time computing system and application .pages 255-262, 2009.

[3] Durresi,A:Barrolli,l cisis 2008, " Secure group communication using battlefield",international conference on complex,intelligent and software intensive system, page 205-210,2008.

[4] Huang y.m.heieh,m.y charo, "pervasive secure access to a hierachical sensor based healthcare monitoring architecture in wireless heterogenous networks",IEEE journel on communication,networking &broadcasting, pages 400-411,2009.

[5] Wenjing lou; Youngoo kwon, " H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks",IEEE transcations on vechicular technology, pages 1320-1330,2006.

[6] Zhou,l ni j: Ravishankar c.v, "Supporting Secure Communication and data collection in mobile sensor network", 25th IEEE international conference on computer communications networking &broadcasting,pages 1-12,2006.

[7] Jyh-ming Huang:shin-chieh tai:kuong-hochen, " A Secure and fault-tolerant data collection scheme using 3-way forwarding and group key management in wireless sensor network", wireless telecommunications symposium, pages 1-6,2009.

[8] Chung skewing, "Secure group communications using key graphs", CISIS 2008 international conference on complex, intelligent and software intensive system, pages 205-210, 2008.

[9] Poornima A.S; Amberker,b.b, " Secure data collection using mobile data collection in clustered wireless sensor networks",IEEE Communication networking &boardcasting,pages 85-95,2011.

[10] Tao shu,sis liu and manwan karunz, " Secure data collection in wireless sensor networks using randomized dispersive routes,IEEE communication networking& boarcasting,pages 2846-2850,2009.