International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 6, June - 2014

Secure Hierarchical Data Aggregation in Wireless Sensor Networks – General Framework

Priti[1], Suman[2]
[1]Deptt. Of Computer Science
G.V.M Girls College, Sonipat, Haryana (India)
[2] Deptt.of Computer Sc. &Engg.,
DeenbandhuChhotu Ram University of Sc. & Tech., Murthal, Sonipat, Haryana (INDIA).

***Abstract* -Secure data aggregation protocol in wireless network has been researched widely over past few years. Wireless sensor network is being used by the military, scientists and civilian such as border security, weather or pollution departments and traffic signals etc. WSN aggregated data could be sensitive and can be misused by hackers or enemies. This may result in falsification of aggregated information which may results in a drone attack on friendly forces in military or traffic jam in city resulting chaos. This paper presents a comprehensive study of several important secure hierarchical data aggregation protocols in WSN.**

Keywords:Wireless Sensor Network, Security, Hierarchical Data Aggregation, Attack, Security Requirements, General Framework

1. INTRODUCTION

Wireless Sensor Network (WSN) are tiny nodes with limited processing power and wireless communication usually positioned in physical or environmental to aggregate sensitive information. These nodes are usually unattended and can be interfered easily with hacker's attacks. Securing tiny wireless nodes is one of the crucial issues in WSN so as to ascertain worthiness of data.

WSN network are usually deployed in unattended areas or where information is required from extreme conditions. The data aggregated from large number of wireless sensor network is always processed with different applications. The crucial decision making applications interfered with malicious data will always result in an incorrect result set. It will be of no use, if advance defense applications with good WSN network at boarder results with incorrect decisions. Also limited available power energy of wireless sensors for data aggregation & integrity if wasted in processing malicious data than no would like to invest or rely on the costly WSN networks.

Therefore, security is an important issue for wireless sensor networks and there are many security considerations that should be investigated in adherence to the application use of WSN. Following are the key factors (application) explains what all are the security problems that tradition network do not face [1].

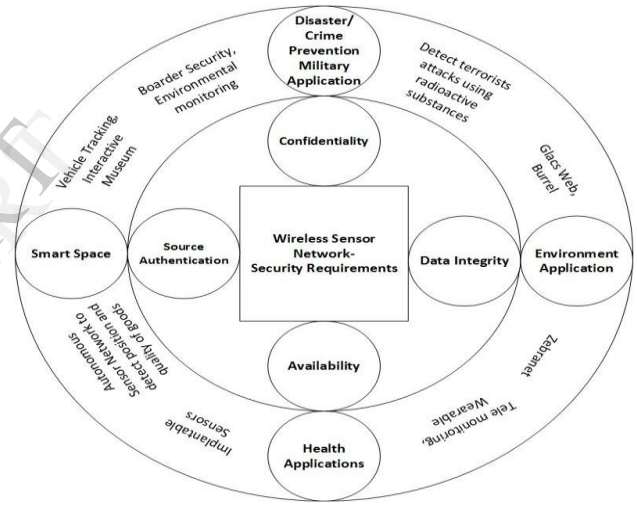

Figure 1. WSN-Security Requirements

WSN security can't be achieved by just implying different security techniques into its protocols. WSN applications are always designed to achieve specific goals and are unique in functionalities. Different WSN applications has been discussed in [1] and resulting different security requirements as shown in figure 1. WSN Data aggregators should able to handle the threat of various types of attacks. Also, secure data transmission needs to be achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. In this paper General Framework of security will be discussed along with protocols for data aggregation in WSN, Security requirement and security issues in hierarchical data aggregation in WSN. The paper has detailed analysis of the security threats, review proposed security mechanisms for wireless sensor networks. It also includes the discussion on the holistic view of security for

ensuring layered and robust security in wireless sensor networks.

The paper is organized in the following section. Section 2 summarizes the various security threats in WSN. Section 3 details the different kind of security requirement and type of threats and possible solution for different layers of OSI model.In Section 4& 5 general frameworks of secure data aggregation protocols explored along with core security technique. Section 6 reviews the state of art of security solution in WSN done in recent year with comparative view. Finally section 7concludes the paper delineating the WSN secure data aggregation general framework comparing different security schemes.

2. SECURITY THREATS IN WSN

Threats to a WSN are described in [2] and classified into the following categories:

- Passive Information Gathering:
- Subversion of a Node
- False Node
- Node Malfunction
- Node Outage
- Message Corruption
- Denial of Service
- Traffic Analysis

3. SECURITY REQUIREMENTS

In WSN, tiny sensor nodes with fixed limited energy can communicates only with energy overheads. Also, most of the time unattended and without tamper resistance WSN's gathers decision making critical informations from the enviornmental or physical conditions. Both application factors and threats results in various security requirements in the WSN's as follows.

1. Authentication – Data from correct sources (sensors)
2. Data Confidentiality -
3. Availability – Energy efficient security algorithms to make network available for long time.
4. Time Synchronization – Accurate and automatic
5. Data integrity – Information has not changed
6. Data Freshness – Recent data, no repeat data
7. Self organization – To conduct key management and building trust relationship among sensors.

With various improvemens now a days, WSN works with smart data aggregation i.e. multiple sensing data by performing diverse operations like algebraic or statistical operations such as addition, median, minimum, maximum, and mean of a data set, etc., which is sensed by sensor nodes. Aggregation accuracy is key in making final decision and is always based on the aggregation result, especially for some sensitive applications where a small difference of result may lead to completely different decisions [3] . Secure hierarchical data aggregation should exists in WSN to remove all the security threats and covring all the security requirements. In WSN secure data aggregation is the key and its protocol should be able to handle the layered attacks (as shown in table 1) with different securtiy approaches.

Layer	**Attacks**	**Security Approach**
Physical Layer	Jamming and tampering	Use spread-spectrum techniques and MAC layer admission control mechanisms
Data Link Layer	Jamming and Collision	Use error correcting codes and spread spectrum Techniques
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	injects false messages and energy drain attacks	Authentication
Application Layer	Attacks on reliability	Cryptographic Approach

*Table 1.*Security Threats and Possible Solutions for Different Layers of OSI Model

4. GENERAL FRAMEWORK OF SECURE DATA AGGREGATION PROTOCOLS

Securing data aggregation in WSN is a broadly used term encompassing the characteristics of different protocols, security schemes and coverage of different type of security threats. General framework of secure data aggregation, first discuss about the how to make clusters for the randomly placed nodes using different protocol in Bootstrapping phase. Second phase will start with the implementation of the clustering of the Data Aggregation in Data Aggregation phase and finally integrity phase to verify the data aggregation.

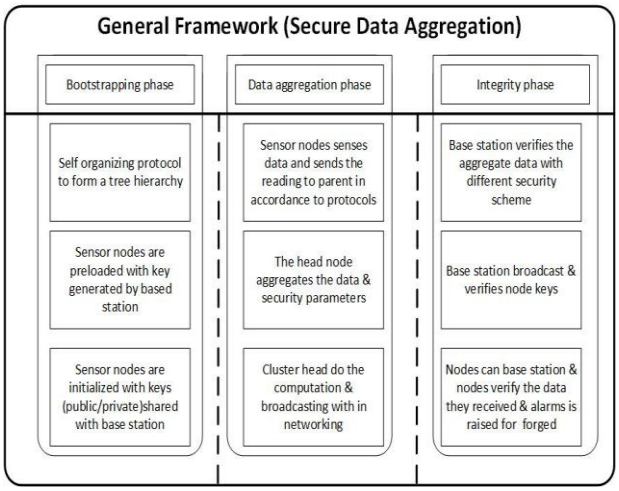

Figure 2. Secure Data Aggregation – General Framework

Any secure data aggregation protocol can be roughly divided into three main phases [12]

Bootstrapping Phase-Bootstrapping phase is the starting phase in WSN. This is all about setting up the network and the keys to carry out secure communication. Different protocols have different steps during the bootstrapping phase. Setting up the cluster head, sharing of security key (public / private), formation of clusters or tree are the primary responsibilities of the phase.

Data Aggregation Phase -Secure the communication between the nodes using the keys obtained in bootstrapping phase using the secure data channels. This can be classified into two groups

- Hop by hop schemes
- End to end schemes

Integrity Phase- This the last phase where base station received encrypted data from the WSN network. It also ensures that any unauthorized party is not able to see the data. The step ensures that any tampering of data can be detected.

5. CORE SECURITY TECHNIQUES

To secure the data aggregation in wireless sensor network, tiny nodes broadcasts should be made authentic and secure. Following are the key background pointers[20] used in various schemes. It has believed that following techniques helps in achieving the security key pointers discussed earlier in the paper.

Elliptic Curve Cryptography- Asymmetric cryptography is widely used now days in distributed environment. These keys are power hungry and should be used very carefully in WSN network.

Homomorphic Encryption- Encryption algorithm holding following properties is called homomorphic encryption.

$$enc\left(a \oplus b\right) = enc\,(a) \oplus enc(b)$$

Two types of homomorphism additive and multiplicative i.e. Elgamal and RSA respectively can carryout operations on ciphertext without need the decryption key. The energy efficient encryption with less computation helps in protecting the decryption key by not exposing it at hostile places.

Digital Signatures- Digital signatures are a digital equivalent handwritten signature in real life. Digital signatures are providing data integrity and non repudiation. In digital signatures it uses something unique signer, which can be verified later. Signer just encrypts the hash using his private key and sends this along with the data to the receiver & verifier uses the same hash function as the signer to find the hash of the data.

Aggregated Digital Signatures- Aggregated digital signatures are widely used in WSN. Sensor nodes share it signing key with the base station during bootstrapping phase and Data and signature keys are aggregated with same and during integration phase base station is able to verify the digital signature.

Merkle Hash Trees - Merkle hash tree is a tree of hashes which is used for integrity verification in wireless sensor networks. Each sensor generates a reading and a hash on that reading .The reading and the hash is then passed on to the parent. The parent generates the hash of the hashes of its children and passes it further up. This continues until the root node of the tree obtains the top hash.

6. STATE OF ART SECURITY SOLUTIONS FOR WSN

In the recent years, secure hierarchical data aggregation in WSN security has been able to attract the attention of a number of researchers around the world. Following section review and map various security schemes proposed or implemented so far for secure hierarchical data aggregation.

SAWN [19] schemes is based on hop by hop encryption. Algorithm is based on the idea of delayed aggregation and delayed authentication for resilience against node compromise, with just a mention of symmetric key cryptography for encryption of data.

Secure DAV[12] clustered based hop by hop encryption scheme is divided into two parts, first part is cluster key establishment (CKE) and the second is the verification of encrypted data.

SDAP [13] scheme is hop by hop encryption with probabilistic technique to divide the tree into smaller groups so as not to place more trust on higher level nodes in the tree.

SHDA[14] hop by hop symmetric key encryption is used in the data aggregation phase and a distributed scheme is used

for integrity verification which aids in reducing congestion near the base station

SHA[15] end to end homomorphic encryption for data confidentiality and aggregate digital signatures for data integrity purposes.

CDA[16] end to end encryption and aggregated signature scheme is based on bilinear maps, with the property that if there are n users and the size of each signature is m, the combined signature is of size m rather than n*m

EDA[17] end to end homomorphic encryption scheme deals with data confidentiality, does not touch upon the data integrity part.

SDA[18] Domingo-Ferrer privacy homomorphism (DFPH)The scheme uses groups inside clusters to have resilience in the event of some nodes being compromised.

Following table shows the detailed comparison of secure data aggregation schemes showing the algorithms used in various phases. EC-PKS refers to Elliptic curve cryptography, EC EG is Elliptic curve EIGamal, DFPH is Domingo-Ferrer privacy homomorphism and EC DSA is Elliptic Curve digital signature algorithm.

Scheme	**Network Model**	**Encryption Scheme**	**Integrity verification scheme**	**Key Distribution scheme**
SAWN[19]	Hierarchical	Symmetric key	MAC	Not Specified
Secure DAV[12]	Clustered	EC-PKC	Merkle Hash Tree(MHT)	Asymmetric group wise Key distribution
SDAP[13]	Hierarchical	Symmetric Key	MHT with a probabilistic	Not Specified
SHDA[14]	Hierarchical	Symmetric Key	Hash Tree	Not Specified
SHA[15]	Hierarchical	ECEG	EC DSA	Not Specified
CDA[16]	Clustered	Mykletun's CDA	Boneh and Gentry	Not Specified
EDA[17]	Hierarchical	Mod stream cipher	Not Specified	Not Specified
SDA[18]	Clustered	DFPH	MHT	Random Key pre distribution

Table 2.COMPARISON OF DIFFERENT Security Algorithms for WSN

CONCLUSION

WSN security requirements are usually driven by its applications and key factors of the purpose of deployment.Each type of security threats are always not required to be handled in every application. Wireless sensor networks, sensor nodes are usually resource inhibited and battery-limited. So these days securityonly aimedfor application as well as in accordance to deployed environment conditions.

Secondly, there are various different secure data aggregation schemes we have discussed. Each of them follows the general framework to secure the data aggregation with various different security primitives as well as secure data aggregation schemes. When reviewed and compared different schemes, it has analyzed how encryption and signing is done at each node while cipher text and signature addition takes place at the aggregators and decryption and verification of data is performed only at the root node.

Again, ensuring absolute security in WSN without taking its application into consideration is still a major research issue. Majority of secure data aggregation schemes are based on specify network model and there is a lack of effort to take a common model to secure WSN at each layer.

In our future work, we plan to extend our work based on hierarchical data aggregation protocols, in order to implement the secure data aggregation and how the algorithm can be used to achieve better performance.

REFERENCES

1. EikoYoneki, Jean Bacon - Technical Paper Number 646 - A survey of Wireless Sensor Network technologies: research trends and middleware's role -UCAM-CL-TR-646 ISSN 1476-2986 September 2005
2. Avancha, S. et al. Wireless Sensor Networks. Kluwer Academic/Springer Verlag Publishers, 2003.
3. Secure Data Aggregation using Ladder Diffusion Algorithm in Wireless Sensor Networks - International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569)-Vinu Raja VijayaKumar[1] S. Chinnaiya
4. A review on data aggrgation (kiranmaraiya,kamalkant,nitingupta)
5. secure data aggregation in wireless sensor networks(suatozdemir,yangxiao)ELSEVIER PAPER
6. A review on data aggregation techniques in wireless sensor network(vaibhavpandey, amarjeetkaur and narottamchand)
7. Security of wireless sensor network(daniel E Burgner and luay A Washeh)2011 IEEE
8. secure reference based data aggregation protocol for wireless senaor network(miriyalamarkandeyulu and guttkondaprashanti)

9. Hu, Y., Perrig, A., & Johnson, D.B. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), vol. 3, pp. 1976-1986, IEEE, San Francisco, CA, April 2003.
10. [2] Paek, J., Chintalapudi, K., &Govindan, R."A Wireless Sensor Network for Structural Health Monitoring: Performance and Experience"2005.
11. Crossbow Technology, Inc., MPR/MIB Mote Hardware Users Manual, http://www.xbow.com/Support/Support_pdf_files/MPR-MIB_Series_Users_Manual.pdf
12. Ajay Mahimkar and Theodore S Rappaport, "SecureDAV: A secure data aggregation and verification protocol for sensor networks" In *Proceedings of the IEEE Global Telecommunications Conference*, 2004.)
13. Yi Yang, Xinran Wang, Sencun Zhu and Guohong Cao, "SDAP: a secure hop-by-hop data aggregation protocol for sensor networks". In *MobiHoc '06: Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing*
14. Haowen Chan, Adrian Perrig and Dawn Song "A Secure Hierarchical In-network Aggrega-tion in Sensor Networks". In *CCS 2006*
15. Julia Albath and Sanjay Madria, "Secure Hierarchical Aggregation in Sensor Networks,". In Proceedings of IEEE Wireless Communications and Networking Conference, 2009
16. Hung-Min Sun, Ying-Chu Hsiao, Yue-Hsun Lin, Chien-Ming Chen, "An Efficient and Verifiable concealed Data Aggregation Scheme in Wireless Sensor Networks" in *Proceedings of the 2008 International Conference on Embedded Software and Systems ,pp. 19-26*
17. C. Castelluccia, E. Mykletun and G. Tsudik. "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks". In MobiQuitous 2005
18. Shu Qin Ren, Dong Seong Kim, Jong Sou Park, "A Secure Data Aggregation Scheme for Wireless sensor Networks" in ISPA Workshops 2007, pp 32-40
19. Lingxuan Hu and David Evans, "Secure Aggregation for Wireless Networks". In *Workshop on Security and Assurance in Ad hoc Networks, 2003.*
20. *Vimal kumar and sanjaymadria," Secure Data Aggregation In Wireless Sensor Network ".*