International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 4.438

Secure and Economical Information Transmission for Clustered Wireless Sensor Network

Kalokhe Komal A.[1], Tamboli Mohasin B.[2]

[1] M.E. Student, G. H. Raisoni College of Engineering and Management, Ahmednagar,414001, India
Savitribai Phule Pune University

[2] Assistant Professor, G.H.Raisoni College of Engineering and Management, Wagholi, Pune,411015, India
Savitribai Phule Pune University

Abstract: ***Now a day's security is a crucial issue in wireless detector network. Cluster is effective means for energy potency. During this Paper we have a tendency to study secure information transfer for stratified WSN. In stratified WSN clusters square measure created dynamically and sporadically. we have a tendency to planned two secure information transmission protocol for stratified WSN, referred to as as SETABE and SET ABOOS, by victimization attribute primarily based coding theme and attribute based on-line offline coding. Throughout information transmission finds orphan node attack, misbehavior of node with the assistance of Diffie-Hellman rule.***

Keywords: Attribute-based Cryptography, Attribute-based online/offline Cryptography, Clustered WSNs, Secure Information Transmission Protocol

1. Introduction

WSN is exacting and huge assortment of distributed detectors nodes known as as sensor devices, that are capableofsensing info like condition, like sound , temperature , motion. Detector node senses environmental conditions and collects information from their domain space, processed them and send towards sink node. Secure information transfer is most crucial issue for WSN. Generally, most of WSNs are deployed with rough, crude, differed physical setting for military and aid domain with trustless background. So, firmly information transmission is critical and most sensible vision in WSN.

2. Background and Motivation

Hierarchical primarily based information transfer in WSN has been researched to realize network quantifiability and maximizes node period and low power consumption with energy economical routing. In stratified WSN each cluster has leader node referred to as as cluster head node (CH). A CH gathered all information that is collected by leaf node in individual cluster. this can be usually referred to as as information aggregation, send combination information to base station (BS)conjointly referred to as as sink node. The LEACH (Low Energy adaptational clump Hierarchy) protocol bestowed by Heinzelmal et. al. [1] is greatly famous effectively wont to cut back total system energy consumption and balanced energy by distributing the energy load haphazardly among all nodes in WSN and support to stratified WSN. In LEACH protocol BS is fastened and situated far from detectors and every one sensor nodes are same in nature. In cluster, one detector node is cluster head (CH) acts as native BS, LEACH haphazardly choose cluster head for energy equalization purpose.

So, all sensors consumes same battery power equally.BS is high energy node and leaf node is low energy node. LEACH performs in rounds, it's 2 phases: Setup part, Steady part. In setup part, clusters square measure created and CH is chosen at random for every cluster, wherever as in steady part leaf node send knowledge to CH inside bound period mistreatment TDMA. The concepts of LEACH protocol, range of protocols are developed like PEACH [3], APTEEN [2] and PEGASSIS [4] that uses same conception like LEACH. During this paper, for our convenience we tend to used form of class-conscious protocol as LEACH protocol. However, implementation of class-conscious primarily based design in globe is difficult. Providing security to LEACH protocol is extremely advanced as a result of the dynamically and sporadically changes network, cluster head of network and knowledge path[8].

Therefore, providing steady and stable node to node sure relationship and customary key distribution isn't possible in LEACH like protocol. There some secure knowledge transmission protocols square measure out there supported LEACH protocol, like SEC-LEACH [6], GS-LEACH [7].But, several of them uses bilaterally symmetrical key management for network security, that suffer from orphan node drawback. This drawback happens once node doesn't share pairwise key with different node in their cluster to serve the storage price of bilaterally symmetrical key. The ring in node isn't able to share pairwise non-public key with all node in network. In such a case, the node can't participate in different cluster. So, that additional CHs square measure non appointive by themselves that ends up in additional energy consume by network [1].The orphan node will increase the overhead of network and also the system energy consumptions by increasing range of CHs in network. to beat bilaterally symmetrical key management, uneven key management has been recently employed in WSN, with Attribute primarily based coding Technique (ABE).

It supported set of attribute that they enforced on cluster of linear attribute set, supported Diffie playwright algorithmic

rule or Elgamal[12]. ABE permits users to write message and decipher message supported users attribute. it's 2 main kind of ABE: Key policy ABE (KP-ABE) and Cipher policy ABE (CP-ABE). during this paper, we tend to projected two protocols supported ABE that's SET-ABE, SET-ABOOS. The ABOOS theme may well be effective for key management, the offline part are often dead on device nodewhereas on-line part dead throughout communication [8].

3. Related Work

Abdul Gani khan & AbdurRohan et al. [4] explicit information transmission protocol for gradable primarily based WSN, like LEACH, TEEN, APTEEN, PEGASSIS. It distribute information as per got to any router that may receive. supported this comparative analysis of protocol is conferred. Online/offline Attribute primarily based cryptography theme mentioned by Susan Honerberger & brent goose water [5].They developed new "correct and connect" technique with 2 parts: preparation phase and online/offline cryptography. This technology cut backs battery power on nodes & reduce bottleneck on master authority task. Huang Lu, Jili et.al. [8] planned two information transmission protocol named as SET-IBS & SET-IBOOS supported Digital Signature to attain security parameter additionally it solve downside of orphan node with symmetrical key management. Attribute primarily based cryptography planned by Sahani and B. Waters [13] they states that identity of user is viewed as cluster of attribute. They verified theme below the Selective-ID model that may be viewed as a changed version of the linear Decisional Diffie-Hellman assumption.

4. Design

WSN consisting of fastened bachelor's degree and every one leaf nodes, that square measure homogenized in nature with same practicality. The bachelor's degree is usually reliable and trustworthy licensed user; wherever the sensing element nodes could compromise by unauthorized user and transmission path could also be interrupted by unauthorized user. In WSN, sensing element nods square measure classified into clusters and each cluster has CH nodes, which might be designated arbitrarily. A Non-CH node (leaf node) joins clusters betting on strength of received signal from bachelor's degree. CH performs information assortment and transmission towards bachelor's degree with high energy than leaf node. The LEACH protocol used for implementation of WSN. Operation of LEACH protocol divided into 2 parts which will be administrated among variety of sphericals every round embrace separate setup part for forming clusters and steady phase for knowledge transmission from detector nodes to SB through CH. Time is split into variety of your time slot, for knowledge transmission and cluster formation it uses TDMA theme. In every around the time line is split into consecutive measure by TDMA management.

Sensor nodes sends detected information to CHs in on every occasion slot of steady section, CHs square measure elective willy-nilly for balance energy and non-Ch detector nodes be a part of clusters victimization 2 hop transmissions reckoning on higher receiving signal. to pick out CH in new spherical every leaf node determines random range and compare with threshold price. If price is a smaller amount than price of threshold then detector node becomes CH for current spherical. this can be the approach for brand new CHs square measure self hand-picked supported their own native call [8].

SET-ABE rule is enforced for secure information transfer in WSN. In has four operations: setup, key Generation, Encryption, Decryption.

1) Set up: The authority user as Bachelor of Science generates master and public key parameter for generation of personal key and send them to all or any detector nodes in cluster.
2) Key Generation: The authority executes and generates non-public key for information user.
3) Encryption: information owner code messages with set of attributes.
4) Decryption: An Information user rewrite the encrypted message with non-public key and verifies receiving output is suitable or not that depends on attribute matching.

5. Conclusion

In this paper, we've style and developed 2 protocol theme so as to induce secure and economical knowledge transfer over WSN, like SET-ABE and SET-ABOOS supported Attribute primarily based cryptography. Additionally because it offer security towards orphan node drawback in secure knowledge transmission. Because of use of stratified design provides balanced energy consumption on each device node

References

[1] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.
[2] Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
[3] S. Yi et al.," PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks " Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
[4] Abdul GaniKhan,AbdurRahman, NeetiBisht "Classification of Hierarchical Based Routing Protocols for Wireless Sensor Networks", International Journal of Innovations in Engineering and Technology, ISSN:2319-1058,Special Issue-ICAECE-2013.
[5] Susan Hohenberger, Brent Waters "Online/Offline Attribute-Based Encryption",2007.
[6] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
[7] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l

Symp.Network Computing and Applications (NCA), pp. 145-152, 2007.

[8] Huang Lu, Jie Li, Mohsen Guzani "Secure and Efficient Data Transmission for Cluster-Based Wireless sensor Networks",IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2004.

[9] Cheng-chi Lee,Pei-Shan chung,and Min-Shiang Hwang "Asurvey on Attribute-based Encryption Scheme of Access Contol in Cloud Environment", International Journal of Network Security, Vol.15,No.4,PP.231-240,July2013.

[10] Susan Hohenberger, Brent Waters "Online/Offline Attribute-Based Encryption",2007.

[11] Susan Hohenberger, Brent Waters "Attribute-Based Encryption with Fast Decryption",8may 2013.

[12] Shraddha U. Rasal,BharatTidake"Improving Revocation Sheme to Enhance the Performance in Multi-Authority ABE",International Journal of computer Application(0975-8887) Vol 90-No 18,March 2014.

[13] Shai and B.Water,"fuzzy Identity based Encryption," Advance in CryptogyaphyEu-rocrypt, LNCS, Spinger, vol.3494, pp.475-473, 2005