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

A Survey on Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks (CWSN)

Vijay Kukre[1], Shubhangi Vairagar[2]

[1]PG Student, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

[2]Professor, Computer Department, Siddhant College of Engineering, Sudumbre, Savitribai Phule Pune University

Abstract: ***Secure data broadcast is a severe problem for wireless sensor networks (WSNs) so the clustering is an efficient and realistic method to get better system performance of WSNs. This paper discussed the secure data broadcast for cluster-based WSNs (CWSNs) where the clusters are created dynamically and periodically. The two proposed Secure and Efficient data Transmission (SET) protocols used in cluster-based WSNs [1] are SET-IBS and SET-IBOOS with the Identity-Based digital Signature (IBS) method and the Identity-Based Online/Offline digital Signature (IBOOS) method, respectively. In SET-IBS, security depends on the rigidity of the Diffie-Hellman problem in the coupling domain. The SET-IBOOS additionally minimize the computational burden for protocol security, which is crucial for WSNs, at the same time as its security depends on the rigidity of the discrete logarithm problem. This paper shows the practicability of the SET-IBS and SET-IBOOS protocols regarding the security requirements and security analysis beside a variety of attacks. The result shows the efficiency of the proposed protocols. In the terms of security overhead and energy consumption, the outcome of the proposed protocols have enhanced performance than the existing secure protocols for CWSNs, In this paper, we discussed a secure data transmission for cluster-based WSNs in which the clusters are formed dynamically and at regular intervals.***

Keywords: Cluster-based WSNs, ID-based digital signature, SET-IBS, SET-IBOOS, LEACH, PEACH, SecLEACH. RLEACH

1. Introduction

Wireless Sensor Network (WSNs) is used in several applications in military sensing such as opponent movement on the battleground or the position of persons in a building and tracking, monitor and record physical or environmental condition, disaster management and biomedical areas which normally include the monitoring of sensitive information. Hence, the security and efficient data transmission is most vital matter in WSNs beside this WSNs go through from many constraint, with low calculation ability, small memory, limited power resources, vulnerability to physical capture, and the utilize of insecure wireless communication channels. Cluster-based data transmission in WSNs has been studied by researchers to accomplish the network scalability and administration, which extends the node lifetime and reduce bandwidth utilization by using local cooperation among sensor nodes. In CWSNs, each cluster has a leader sensor node acts as cluster head (CH) who aggregates the data collected by the other nodes called as non-CH sensor nodes in its cluster, and forwards the aggregation to the base station (BS).

The (LEACH) protocol with low-energy adaptive clustering hierarchy [2] is a efficient one to reduce and balance the entire energy consumption for CWSNs. To avoid rapid energy consumption of the set of CHs, LEACH at random rotates CHs within all sensor nodes in the network, in rounds. LEACH achieves improves the network lifetime.

The LEACH protocol dynamically, randomly, and periodically reorganizes the network"s clusters and data links which adds security challenge to LEACH-like protocols. Therefore, providing stable long-term node-to-node trust relationships and common key distributions are insufficient for LEACH-like protocols. Nevertheless, pertain the symmetric key management for security, which suffers from a orphan node problem which occurs when a node does not share a pair wise key with others in its preloaded key ring.

So, to overcome this issue, this paper introduces the two proposed Secure and Efficient data Transmission (SET) protocols for cluster-based WSNs [1] are SET-IBS and SET-IBOOS with the Identity-Based digital Signature (IBS) method and the Identity-Based Online/Offline digital Signature (IBOOS) method, respectively.

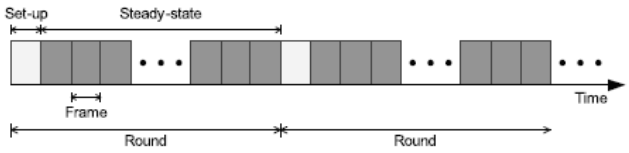

Figure 1: Operation of proposed secure data transmission

Once the protocol is initialized, SET-IBS works in rounds during communication. Each round has two phases i.e. a setup phase and a steady-state phase. The process of SET-IBS is divided by rounds as shown in Fig. 1, which is same like to other LEACH-like protocols. Every round consists a setup phase to form clusters from CHs, and a steady-state phase to transmit data from sensor nodes to the BS. The timeline is divided into consecutive time slots by the TDMA control in each round [2]. In steady state phase, sensor nodes forward the sensed data to the CHs in each frame. The nodes are randomly selected as CHs in every round for efficient energy consumption, and other non-CH sensor nodes connect clusters using one-hop transmission, only on receiving the

highest received signal strength of CHs. To select CHs in a next round, every sensor node fixes a random number and compares it with a threshold. The sensor node is selected as a CH for the current round if the value is less than the threshold. Thus, the new CHs are self-selected based by the sensor nodes themselves only on their local decisions; so, SET-IBS operates exclusive of data transmission with each other in the CH rotations.

2. Literature Survey

In paper [2], they develop and assess low-energy adaptive clustering hierarchy (LEACH), protocol architecture for micro-sensor networks which integrate the ideas of energy-efficient cluster-based routing and media access jointly with application-specific data aggregation to get excellent performance with respect to system lifetime, latency, and application-perceived quality. LEACH provides algorithms for adapting clusters, a new, distributed cluster configuration technique which provides self-organization of huge numbers of nodes and rotating cluster head positions to uniformly distribute the energy load between all the nodes, and techniques to provide distributed signal processing to save communication resources. The results prove that LEACH can enhance the system lifetime with respect to magnitude as compared with general-purpose multi-hop methods. The *disadvantage* of LEACH is that sensors must broadcast data to the cluster head during their allocated TDMA slot continuously so it does not save energy consumption. While implementing LEACH, all nodes are inside the communication range of each other and the Base Station but this limits the scalability of the protocol. The *advantage* is that the cluster head position rotates among all nodes by ensuring that requires the lowest transmitting power reduces energy dissipation and latency in data transfer.

Figure 2: Time line showing LEACH operation

The working process of LEACH is split up into *rounds and* each round starts with a set-up phase where the clusters are arranged, next a steady-state phase in which data are forwarded from the nodes to the cluster head and BS, as shown Fig. 2.

In paper [3], they propose PEACH protocol that is a power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. The PEACH protocol makes the clusters with no additional burden and provides adaptive multi-level clustering and also can be used for both location-unaware and location-aware wireless sensor networks. The PEACH considerably minimizes energy utilization of each node and increases the network life span, as compared to existing clustering protocols. The performance of PEACH is not much so affected by the distribution of sensor nodes as compared to other clustering protocols. The advantages of PEACH protocol are that it provides longer network lifetime, smaller and unbiased energy consumption, and better scalability as compared to existing clustering protocols and also support the adaptive multi-level hierarchical clustering The disadvantage of this protocol is it does not provide security.

In paper [4], initially they study the problem of adding security to cluster-based sensor networks where clusters are created dynamically and periodically for LEACH protocol. So efficient security communications in LEACH protocols, they have proposed SecLEACH, protocol which is customized version of LEACH which uses random key pre-distribution and μTESLA which provides authenticated broadcast to secure hierarchical WSNs with dynamic cluster configuration with rotating CHs. Here they have solved the orphan node problem by adding small protocol which allows the „already adopted children" to bring back the orphans node into their clusters. The numbers of orphan nodes impact on the performance of the network. As SecLEACH does not provide pair-wise communication so, the biggest security issue in SecLEACH is possible to be its resiliency not in favour of node captures. In SecLEACH, due to the constraints forced by key sharing, not all CHs are reachable to all ordinary nodes.

In paper [5], they study adding security to cluster-based routing protocols for wireless sensor networks which consisted of sensor nodes with harshly restricted resources, so they suggest a security solution for LEACH a protocol where the clusters are formed dynamically and periodically. The solution provided by authors use enhanced Random Pair-wise Keys (RPK) method based on probability, a definite number nodes shared key are stored in each node's memory, ensuring network's connectivity by keeping probability of connection. The optimized security method that depends on symmetric key methods which shows that security of RLEACH has been enhanced, with reduction in energy utilization and very less operating cost. The disadvantages of RLEACH are, larger number of groups lead shorter lifetime as it establishes security mechanism by means of key management which increase the energy consumption. Secondly, if smaller the number of groups, it decreases the energy consumption of establishing shared-key but reduce the security.

A serious security need is authentication to avoid attacks against secure communication in Wireless Sensor Networks (WSNs) and to reduce DoS attacks use the limited resources of sensor nodes. Resource restraint of sensor nodes are main trouble while applying strong public key cryptographic based mechanisms in WSNs. To deal with the problem of authentication in WSNs, in paper [6] they have proposed secure and efficient structure for authentic transmission by sensor nodes and for external user authentication, which uses identity based online/offline signature schemes. The main purpose of this structure are to allow all sensor nodes in the network, initially, to transmit an authenticated message speedily; secondly, to confirm the transmitted message sender and the message contents; and lastly, to confirm the authenticity of an external user. The projected structure is also evaluated by the most secure and efficient identity-based signature (IBS) schemes.

The main advantage of this system is its re-usability means reused with new IBS and IBOOS schemes for security to

improve the performance. But it does not provides user access control to provide a complete ID-based authentication framework

The clusters are formed periodically and dynamically in secure routing for cluster-based sensor networks. By studying the ID-based cryptography for security in WSNs, in paper [7], authors proposed a new secure routing protocol with ID-based signature method for cluster-based WSNs in which the security is reliant on the rigidity of the Diffie-Hellman problem in the random oracle model. Here the insufficiency in the secure routing protocols using symmetric key pairing is pointed by authors. Because of the communication operating cost for security, authors provide simulation investigation results to reveal how a variety of parameters operate among energy efficiency and security.

The disadvantage of the proposed protocol is that sensor node consumes energy faster than LEACH protocol because communication burden and the pairing computation cost for ID-based digital signature.

In paper [8], they study the routing problems for WSNs and proposed a novel energy efficient cluster-based routing algorithm for hierarchical WSNs where sensor nodes are hierarchicalized into different levels by using the hop number of transmissions to the base station. Cluster-head sensor nodes are chosen autonomously and broadcast data to the base station using multi-hop transmissions, while non-cluster-head sensor nodes communicate with cluster-head sensor nodes directly. After performing comprehensive simulation experiments using proposed algorithm, the simulation results shows that it increases network lifetime and also mitigates the outcome of self-induced black hole and balance the energy usage in the network by employing alternative sensor nodes. This proposed algorithm does not provide the secure data transmission as they are not talking about security.

3. Conclusion

In literature survey discussed different protocols LEACH, PEACH, SecLEACH and LEACH with Random Pair-wise Keys (RPK) known as RLEACH, Identity-Based Signatures LEACH. In this paper, the drawback of the symmetric key management for secure data transmission has been reviewed followed by the study of two secure and efficient data transmission protocols for CWSNs, i.e. SET-IBS, and SET-IBOOS.

SET-IBS and SETIBOOS protocols are efficient in communication with the ID-based cryptography system, which achieves security needs in CWSNs and also solved the orphan node issue in the secure transmission protocols with ID information and digital signature for authentication. Hence the SET-IBS and SET-IBOOS protocols give better performance as compare to existing secure protocols for CWSNs. The SET-IBOOS has less auxiliary security overhead in term of computation, storage and communication costs for secure data transmission in CWSNs which results to less energy utilization and increase the network life span. Also as compare to other protocol, the network scalability is comparatively high.

References

[1] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE Transactions On Parallel and Distributed Systems, VOL. 25, NO. 3, March 2014

[2] 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.

[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] L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.

[5] K. Zhang, C. Wang, and C. Wang, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,” Proc. Fourth Int‘l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.

[6] R. Yasmin, E. Ritter, and G. Wang, “An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures,” Proc. IEEE Int‘l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[7] H. Lu, J. Li, and H. Kameda, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature,” Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[8] H. Lu, J. Li, and G. Wang, “A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks,” Proc. Fourth Int‘l Conf. Frontier of Computer Science and Technology (FCST), pp. 565-570, 2009