Ensure and Energy Efficient Data Forwarding in Cluster Based Wireless Sensor Network

Priyanka.S[1] Sivakumar.P[2] Thamaraiselvi.K[3] Prakash.M[4]
[1]Student of M.E [2,3,4]Assistant Professor
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]KSR College of Engineering, Anna University, Namakkal, Tamilnadu 637215, India

Abstract— Secure data transmission is a critical issue in wireless sensor networks where clustering is an effective and practical way to enhance the system performance. Two secure and efficient data transmission for cluster based wireless sensor networks called SET-IBS and SET-IBOOS are used. In SET-IBS (Identity Based Digital Signature), the security relies on the hardness of Diffie-Hellman problem in the paring domain. In SET-IBOOS (Identity Based Online/Offline Digital Signature), it reduces the computational overhead for protocol security. To overcome this problem, two protocols MD5 and EARP scheme is used. MD5 algorithm provides the security for data sending between cluster members to cluster head. Energy Aware Routing Protocol is used to choose the effective cluster head as high receiving capabilities in cluster group to improve the life time of the network.

Key words: Cluster based WSN, Identity based digital signature, Identity based digital signature, Message Digest, Energy aware routing protocol

I. Introduction

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensor nodes to monitor the environmental conditions. A WSN typically consists of a sink node which is referred as Base station and a number of small sensor nodes. The information is collected from the sensor nodes and sends to the base station. The collected information is aggregated and the aggregation reduces the amount of network traffic. The main characteristics of the sensor nodes include power consumption, mobility of nodes and cross layer design. The main challenges or issues are occurred in wireless sensor network depend on the real world environments. Most of the protocols are supported to overcome the problem which arises from the challenges. In wireless sensor networks, secure data communication is inadequate.

The Cluster based data transmission in wireless sensor network is mainly to achieve the network scalability and to reduce the bandwidth consumption. In Cluster based Wireless Sensor Network (CWSN) each and every cluster has a Cluster Head (CH) which is a leader sensor node. The cluster head collects and aggregates the data from the cluster members. The aggregated data is then forwarded to the base station.

For secure data communication between the cluster members to cluster head, there are several protocols are used. In addition with security, providing an efficient data transmission is inadequate. For secure and efficient data transmission, digital signatures and LEACH like protocols are used in the existing and more existing solutions are provided for distributed wireless sensor network. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. Low Energy Adaptive Clustering Hierarchy (LEACH) is a TDMA (Time Division Multiple Access) based protocol which is integrated with clustering algorithms and simple routing protocols in wireless sensor network. LEACH is used to reduce and balance the energy consumption of the network. Adding the security in leach like protocols is difficult because it randomly and dynamically rearranges the clusters and the links.

For security in cluster based wireless sensor network, digital signatures are one of the most critical security service offered by asymmetric key management. The SET-IBS (Identity Based Digital Signature) and SET-IBOOS (Identity Based Online and Offline Digital Signature) are used in cluster based wireless sensor network. The public key and the identification of the signer will be obtained as a digital certificate. This will be sent for the receiver for the identification of the sender. This can be proposed to reduce the computation and the storage cost. In IBOOS scheme, the offline phase can be executed at the base station prior to communication and the online phase will be executed during the communication.

In SET-IBS, the security relies on the hardness of the Diffie-Hellman problem in the pairing domain and in SET-IBOOS further reduces the computational overhead for protocol. The security for SET-IBOOS relies on the hardness of discrete logarithmic problem. The protocol is to be initialised and SET-IBS is divided into rounds and each round has a setup phase and steady phase. The setup phase is for the formation of clusters and the steady phase is for the transmission of data from sensor nodes to base station. At each phase the timelines is divided into timeslots by TDMA control. The sensor nodes transmit the sensed data to the cluster head in steady state phase. The nodes randomly select the cluster head and the other nodes act as the cluster member. This will be done for the one hop transmission of data from CH to the sensor nodes.

In the previous protocols, the secret keys and the paring parameters are preloaded and distributed initially in all the sensor nodes. This will leads to the high energy consumption and storage cost is high. By applying the asymmetric key management, for security, the orphan node problem will occurs and the offline phase does not use any secret information for signing. In this paper we propose a new secure and efficient data transmission based protocol to improve the network lifetime. MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input which may be a message of any length. Energy Aware Routing Protocol is used to improve the network performance and is used to choose the effective cluster head as high receiving capabilities in cluster groups.

II. RELATED WORK

Clustering is an effective and efficient way to improve the performance of the network in cluster based wireless sensor networks. Huang Lu [1] used digital signatures for the security in CWSN. It relies on the hardness of the Diffie-Hellman problem and discrete logarithmic problem. The operation of the SET protocols contains setup phase and steady state phase where the computation cost is high.

Karlof [3] used the secure routing protocols for the wireless sensor networks where certain attacks like wormhole and sinkhole attacks are not protected. Randomly virtual base stations are created and data transmission can be done. The virtual base stations are not secure as the transmission between the cluster group and the base station in CWSN.

Zhang [9] used group key management for security in cluster based wireless sensor networks. Random pair-wise keys are distributed in all the sensor nodes. The keys are preloaded in all the sensor nodes before the data transmission. This will leads to high energy consumption of the network. Most of the protocols are designed for multi-hop communication and not suitable for cluster based wireless sensor networks.

Yasmin et al [10] proposed a new framework for paring free IBOOS (Identity Based Online and Offline Digital Signature) for asymmetric key management for wireless sensor networks. This could be expensive for the paring based cryptography. For key management based cryptosystem, for security purpose uses the information and digital signature for verification.

Researchers have proposed many key management schemes, but most of them were designed for flat wireless sensor networks, which is not fit for cluster-based wireless sensor networks (e.g. LEACH). The cluster head in the cluster performs data aggregation and consumes more energy. The CH selection will be made by rotating the cluster members at a randomized manner. By performing this process the low energy nodes are selected as the cluster head, it has the chance of node failure. To avoid this problem, the more energy power nodes is selected as the cluster head.

III. MD5 ALGORITHM

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input which may be a message of any length.MD5 operates in 5 steps where the data is converted to hashed data. The five steps are append padding bits, append length, initializing MD buffer, processing message in 521 bit blocks, output. The original data is appended with padding bits and converted to 64 bits of message blocks.MD5 offers much more assurance of data security than MD4.

MD5 accepts the message as input and generates a fixed length of output. The fixed length output is generally less than the length of input message. The output is called the Hash Data. MD5 can be fast for the 32 bit machines.

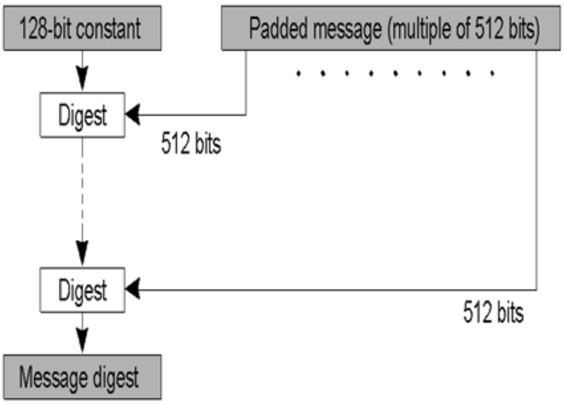

Fig. 1: Working of MD5

A. Hash Data Generation:

The original message is extended that its length is congruent to 448, modulo 512.The data from the cluster member is padded with one bit first and converted to 64 bit blocks. In append length, the length of the original message and the padding bits are calculated for the hash data generation. The length of the original data can be decrypted after the secure communication. The 64 bits are appended at the end of the padded bits to indicate the original length of the data in bytes. In initializing MD buffer, the algorithm requires a 128 bit buffer and the buffer is divided into 32 bits each. The processing of message in 512 bit blocks which contain the loops throughout the padded and appended bits. Then the contents in the buffer can be returned in a sequence of low order byte.

IV. IMPROVED EARP PROTOCOL

The Energy Aware Routing Protocol (EARP) is used to improve the energy of nodes while transferring data from the cluster members to cluster head. The operation of EARP is divided into rounds while each round begins with a set-up phase. The clusters are organized and it chooses the more energy power node as the cluster head. The Cluster head collects the secure data from cluster members and send it to the destination. The main objective of this EARP protocol is to improve the energy of the network. The EARP further introduces the idea of area coverage which is used to reduce the number of working nodes within cluster. This will helps to prolong the network lifetime. It is a novel energy efficient data gathering protocol with the intra-cluster coverage. Energy Aware Routing Protocol clusters the sensor nodes into groups and builds routing tree among the cluster heads for energy saving communication.

A. CH –Selection:

The CH -SELECTION consists of several clustering algorithms for the cluster head selection. The clustering algorithm should be completely distributed because it is in a centralized manner. Among the clusters, the cluster head should be well distributed. The monitoring area is to make the energy consumption and to be well-balanced among all the sensor nodes. The entire clustering algorithm itself should be energy efficient. The battery capacity of all the sensor nodes is not same. The amount of energy consumed in gathering the data will differs among the cluster head. It depends on the number of cluster members and the positions in monitoring area. The energy consumption differs among cluster members due to different distances.

The redeployment for prolonging the network lifetime will cause the residual energy. The residual energy is also not equal among all the sensor nodes. The selection of cluster head primarily depends on the residual energy. The probability of a sensor node's being selected as a cluster head primarily depends on its own residual energy. It does not help to balance the energy load.

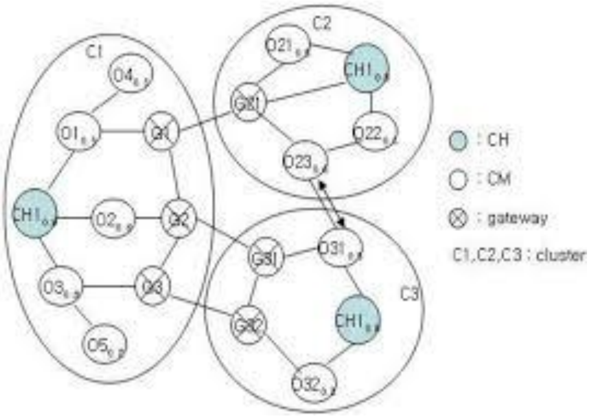

Fig. 2: Example of CH selection

B. *Active Member Nodes Selection:*

The active member node selection is the area coverage area and it is one of the most important issues in Wireless Sensor Networks. The K-coverage can be explained at every point in monitoring field and it is covered by at least K sensor nodes. The more energy node is selected as the cluster head among the sensor nodes.

It is very hard to guarantee the full coverage for the randomly deployed area even if all the sensor nodes are busy in monitoring the area. The active nodes are included in the cluster where the nodes are in distributed manner. The distance between the sensors nodes are also considered as the major issue in active member selection. Coverage mechanism is to choose a subset of active nodes to maintain the coverage expectation.

V. DECISION TAKEN

In this model, we are going to analyze the effective transmission of secure data within the clusters. The performance at each round will be calculated as the high energy receiving nodes. The comparison between the existing and the proposed protocols can be made and routing tree can be constructed. The graph will be constructed with the comparison results and simulation results.

VI. CONCLUSION

In this paper, for secure and energy efficient data transmission, MD5 algorithm and EARP protocol is used. MD5 algorithm provides the security for data sending between cluster members to cluster head and EARP protocol is used to choose the effective cluster head as high receiving capabilities in cluster groups. MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input which may be a message of any length. Energy Aware Routing Protocol is a novel energy efficient data gathering protocol with intra-cluster coverage. EARP clusters the sensor nodes into groups and builds a routing tree among cluster heads for energy saving communication. In addition, EARP introduces the idea of area coverage to reduce the number of working nodes within cluster in order to prolong network lifetime. It shows that EARP outperforms far better than LEACH like protocols. The proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

VII. ACKNOWLEDGMENT

I extend my sincere thanks to my institution, 'K.S.R. College of Engineering' for giving me the opportunity to write a research paper. A special thanks to my Head of the Department, Dr. A.Rajiv Kannan for encouraging us and to Dr.P.Sivakumar for his support and valuable guidance throughout this project work and makes this project as a successful one. Finally, I would like to thank authors of the various research papers that I have referred to, for the completion of this work.

REFERENCES

[1] Huang Lu, Jie Li, Mohsen Guizani,"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] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous), pp. 109-117, 2005.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.

[4] D.Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '01), pp. 213-229, 2001.

[5] 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.

[6] 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.

[7] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.

[8] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

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

[10] 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.

[11] S.Sharma and S.K. Jena, “A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks,” Proc. Int’l Conf.Comm., Computing & Security (ICCCS), pp. 146-151, 2011.

[12] S. Xu, Y. Mu, and W. Susilo, “Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security,” Proc. 11thAustralasian Conf. Information Security and Privacy, pp. 99-110, 2006.

[13] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies inComputational Intelligence, vol. 278. Springer-Verlag, 2010.

[14] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Comm. Surveys &Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[15] Y. Jia, L. Zhao, and B. Ma, “A Hierarchical Clustering-Based Routing Protocol for Wireless Sensor Networks Supporting Multiple Data Aggregation Qualities,” IEEE Trans. Parallel & Distributed Systems, vol. 4, nos. 1/2, pp. 79-91, 2008.