Volume 1, Issue 4, July 2016 ISSN: 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

An Overview on Digital Signature Based Secure Data Transmission for Cluster WSN

Ms. Gauri P.Heda
Dept. of Computer
S.N.D.C.O.R.C,Yeola,Dist-Nashik
Maharashtra, India

Prof. Imran R. Shaikh
Dept. of Computer
S.N.D.C.O.R.C, Yeola,Dist-Nashik
Maharashtra, India

Abstract: ***For wireless sensor networks (WSNs), secure data transmission is a critical issue. To enhance the system performance of WSNs, Clustering is an effective and practical way. Where the clusters are formed dynamically and periodically, we study a secure data transmission for cluster-based WSNs (CWSNs). By using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively, We propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS. in the pairing domain, In SET-IBS, security relies on the hardness of the Diffie-Hellman problem. which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem, SET-IBOOS further reduces the computational overhead for protocol security. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. To illustrate the efficiency of the proposed protocols, the calculations and simulations are provided. In terms of security overhead and energy consumption, the results show that the proposed protocols have better performance than the existing secure protocols for CWSNs.***

Keywords: Cluster-based WSNs, ID-based digital signature, ID-based online/offline digital signature, secure data transmission Protocol.

I. INTRODUCTION

Using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion, AWIRELESS sensor network (WSN) is a network system comprised of spatially distributed devices. The information data locally, and sending data to one or more collection points in a WSN, The individual nodes are capable of sensing their environments, processing. The most important issues for WSNs, efficient data transmission are one. Such as military domains and sensing tasks with trustless surroundings, Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications. Especially necessary and is demanded in many such practical WSNs, Secure and efficient data transmission (SET). AWIRELESS sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1]. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

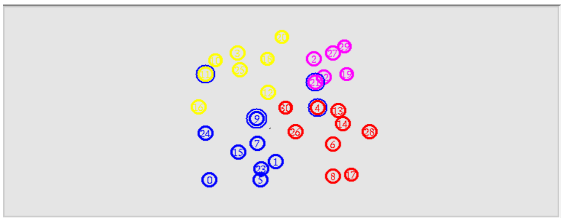


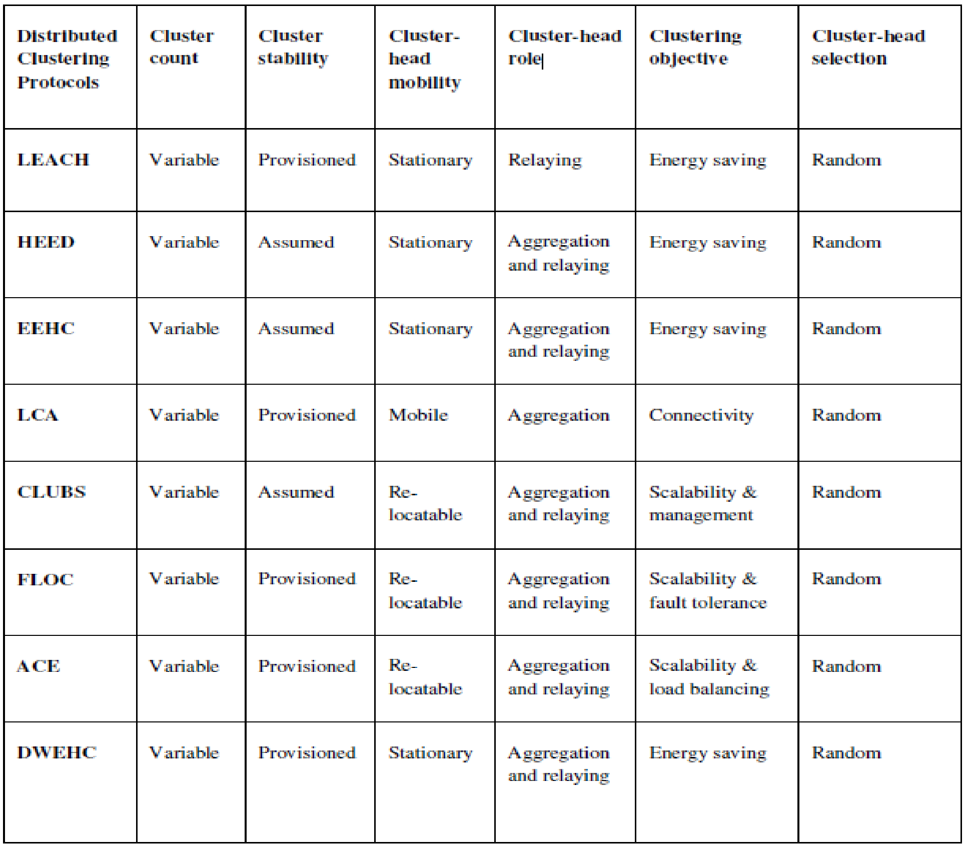
Fig.1 Deployment Of Wsn

A. Background and Motivations

Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes [3]. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). In Wireless Sensor Network the clustering is achieved for Network Scalability and Management which increase the lifetime of the sensor node and reduces the energy consumption. In the clustered Wireless Sensor Network, every cluster has a Cluster Head (CH) and the remaining nodes in the cluster are Leaf Nodes (Non Cluster Head Sensor Node), the data aggregated by the Leaf Node (Non Cluster Head Sensor Nodes) sends to the Cluster Head (CH) and the Cluster Head (CH) then transmits the data to the Base Station. The Low Energy Adaptive Cluster Hierarchy (LEACH) is most probably used for Low Energy Consumption of sensor node in Wireless Sensor Network. To avoid the quick energy consumption of CH's the LEACH protocol will randomly rotates the CH's among the sensor nodes which will leads to improving the Network lifetime. The Protocols which are similar to LEACH are APTEEN and PEACH.

II. RELATED WORK

In Wireless Sensor Network the clustering is achieved for Network Scalability and Management which increase the lifetime of the sensor node and reduces the energy consumption. The Low Energy Adaptive Cluster Hierarchy (LEACH) is most probably used for Low Energy Consumption of sensor node in Wireless Sensor Network. To avoid the quick energy consumption of CH's the LEACH protocol will randomly rotates the CH's among the sensor nodes which will leads to improving the Network lifetime. The Protocols which are similar to LEACH are APTEEN and PEACH. Implementing Security to the LEACH like protocol is the challenging because the data link and Network Clusters are dynamically, randomly and periodically rearranged. So the common key distribution and Node to Node trust was lacking in the protocols like LEACH (The distributed Wireless Sensor Network are existing solution but not for the Clustered Wireless Sensor Network (CWSN). The most similar protocols to LEACH like protocol are SecLEACH, GS-LEACH and RLEACH, these protocols are most probably uses symmetric key management for security in which will cause so called orphan node problem. The orphan node is a problem in which any node which does not share the pair wise key with the other nodes in the preloaded key ring.



Distributed Clustering Protocols	Cluster count	Cluster stability	Cluster-head mobility	Cluster-head role	Clustering objective	Cluster-head selection
LEACH	Variable	Provisioned	Stationary	Relaying	Energy saving	Random
HEED	Variable	Assumed	Stationary	Aggregation and relaying	Energy saving	Random
EEHC	Variable	Assumed	Stationary	Aggregation and relaying	Energy saving	Random
LCA	Variable	Provisioned	Mobile	Aggregation	Connectivity	Random
CLUBS	Variable	Assumed	Re-locatable	Aggregation and relaying	Scalability & management	Random
FLOC	Variable	Provisioned	Re-locatable	Aggregation and relaying	Scalability & fault tolerance	Random
ACE	Variable	Provisioned	Re-locatable	Aggregation and relaying	Scalability & load balancing	Random
DWEHC	Variable	Provisioned	Stationary	Aggregation and relaying	Energy saving	Random

Table1: Comparison of Clustering Algorithm

III. LITERATURE SURVEY

The wireless sensor networks have wide processing capacity in which the data transmission plays a vital role in WSN. We are enhancing a system to have a better data transmission rate. Based upon the study we found that the transmission of data in the Military is still not highly secure. So our system enhancing the security based on the Digital Signature and the security under digital signature. Initially we group the nodes in the form of cluster and those clusters have the cluster head to access the region. After the formation of the cluster region, need to analyze the mobility, and therefore to process the data transmission. For the transmission of data we propose the algorithm EEDC in the existing they have used LEECH. Being the process in wireless network, clusters are formed periodically and dynamically. In the security part we are using two ways, one is the identity based digital signature and Identity based online/offline Digital Signature. So the system will be much more secure than the present strategy. The attacker can be easily identified with this network. Sensors have become a very trendy research area during the last few years covering a wide range of applications such as habitat monitoring, military surveillance, information collecting etc...Sensors used for these purposes needs to be deployed very densely and in a random fashion. They should be able to operate without human intervention. Clustering is a technique employed to increase the various capabilities of a sensor network. In this paper we discuss about the design and implementation issues of clustering algorithms employed in sensor networks.

In Wireless Sensor Network adding security is a crucial issue, the system performance is improved by clustering the Network. The Clustering are formed periodically and dynamically by using Position based Aggregator Node Election for Wireless Sensor Network (PANEL). We propose two protocols called SET-IBS and SET-IBOOS using Id-Based Digital Signature and ID-Based Online-Offline Digital Signature respectively which will add the authentication to the sensed data. For Security the data is encrypted at sender (Leaf Node) and Decrypted at receiver (Base Station). The Security is analyzed by investigating various attacks are Passive Attack, Active Attack, and Node Compromising Attack. The Calculating and Simulation show the efficiency and security of the protocol and the result also shows that the proposed protocol have better performance and security than the Existing Protocols. Wireless Sensor Networks (WSNs), is one of the most rapidly growing scientific domain. This is because of the development of advanced sensor nodes with extremely low cost and the potential applications of such sensor nodes are ever growing. WSNs are web of sensor nodes with a set of processors and limited memory unit embedded in it. Reliable routing of packets from sensor nodes to its base station is the most important task for these networks. Routing in WSN is bit more complex than other wired or wireless networks. The conventional routing protocols cannot be used here due to its battery powered nodes. To support scalability, energy efficiency and efficient routing, nodes are often grouped in to non-overlapping clusters. This paper gives a crisp introduction on clustering process in WSNs. The survey of different distributed clustering algorithms (adaptive clustering algorithms) used in WSNs, based on some metrics such as cluster count, cluster stability, cluster head mobility, cluster head role, clustering objective and cluster head selection is done. The study concludes with comparison of few distributed clustering algorithms in WSNs based on these metrics. Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article we present a survey of security issues in WSNs. First we outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. We then present a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection.

IV. METHODOLOGY USED

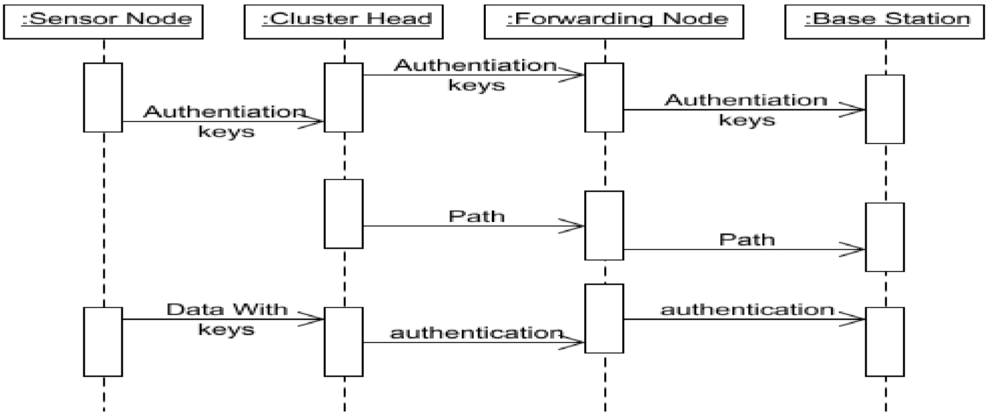


Fig 1: Proposed Method

We propose two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based cryptosystems. Secure communication in SET-IBS relies on the ID based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. SET-IBOOS is proposed to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. We show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations, respectively, with respect to both computation and communication.

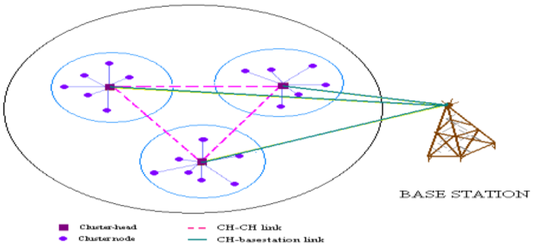


Fig. 3-: Schematic diagram of clustering mechanism.

CONCLUSION AND FUTURE WORK

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SETIBOOS are efficient in communication and applying the IDbased cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

REFERENCE

1. T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
2. 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.
3. A.A. Abbasi and M. Younis, “A Survey on Clustering Algorithms for Wireless Sensor Networks,” Computer Comm., vol. 30, nos. 14/ 15, pp. 2826 2841,2007.
4. 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.
5. A. 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.
6. 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.
7. K. Pradeepa, W.R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” Int’l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.
8. L.B. Oliveira et al., “SecLEACH-On the Security of Clustered Sensor Networks,” Signal Processing, vol. 87, pp. 2882-2895, 2007.
9. 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.
10. 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.
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. G. Gaubatz et al., “State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks,” Proc. IEEE Third Int’l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.