International Journal of Sciences & Applied Research

www.ijsar.in

Comparative Analysis of Secure and Economical Data Transmission for Cluster-Based Wireless Sensor Networks

Bhimashankar K. Dhurape*, Swati S. Joshi

Department of Computer Science and Engineering, N. B. Navale Sinhgad College of Engineering, Solapur, Maharashtra, India.

Correspondence Address: *Bhimashankar K. Dhurape, Department of Computer Science and Engineering, N. B. Navale Sinhgad College of Engineering, Solapur, Maharashtra, India.

Abstract

Secure data transmission could be an important issue for wireless sensing element networks (WSNs). Clustering is an effective and feasible way to inflate the system performance of WSNs. During this paper, we tend to study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formulated dynamically and periodically. We propose two secure and economical data transmission (SET) protocols CWSNs, referred to as SET-IBS and SET-IBOOS, by victimization the identity-based digital signature (IBS) theme and also the identity-based online/offline digital signature (IBOOS) theme, severally. In SET-IBS, protection depends on the hardness of the Diffie-Hellman downside within the pairing domain. SET-IBOOS any reduces the machine overhead for protocol security that is crucial for WSNs, whereas its security depends on the hardness of the discrete logarithm problem. We show the feasibleness of the SET-IBS and SET-IBOOS protocols with relevance the safety necessities and security analysis against numerous attacks. The calculations and simulations square measure provided as an example the potency of the papered protocols. The results show that the papered protocols have higher performance than the prevailing secure protocols for CWSNs, in terms of protection overhead and energy consumption.

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

Introduction

A Wireless sensor network (WSN) is a system of network comprised of spatially dispersed devices using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and movement. The individual nodes are competent of sensing their environments, processing the information statistics in the vicinity, and sending data to one or more compilation points in a WSN. Efficient transmission of data is one of the most significant tissues for WSNs.

Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. Efficient and secure transmission of data is thus very essential

and is required in much such realistic WSNs. Cluster-based transmission of data in WSNs, has been examined by researchers in order to accomplish the network scalability and supervision, which maximizes node life span and reduces bandwidth utilization by using local cooperation between sensor nodes.

In a cluster-based WSN (CWSN), each cluster has a leader sensor node, regarded as cluster head (CH). The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman et al. [4] is a broadly known and effective one to reduce and balance the total energy consumption for CWSNs.

Adding security to LEACH-like protocols is difficult as a result of they dynamically, randomly, and periodically set up the network's clusters and knowledge links [8]. Therefore, providing steady durable node-to-node trust relationships and same key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, however not for CWSNs). There are some secure knowledge transmission protocols supported LEACH-like protocols, like SecLEACH [8], GS-LEACH [11], and RLEACH [12]. Most of them, however, apply the regular key management for security that suffers from a questionable orphan node downside [7]. This downside happens once a node doesn't share a pairwise key with others in its preloaded ring.

Literature survey

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Data Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010; we compare IBOOS with two recently proposed anonymous geographic routing protocols: AO2P and IBS which are based on hop by hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare IBOOS with the baseline routing protocol GPSR in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination. In IBS, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a sec urea map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route.

[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;A wireless sensor network is a special kind of Ad -hoc network, consist of thousands of small devices which are called as sensor nodes used to monitor physical or environmental conditions Clustering is a critical task in Wireless Sensor Networks for energy efficiency and network stability. In the existing method, a secure data transmission for cluster-based WSNs is presented in which the clusters are formed in a dynamic and periodic manner. A two secure and efficient data transmission protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS, by using the identity -based digital signature (IBS) scheme and the identity -based online/ offline digital signature (IBOOS) scheme, respectively. But the drawback in the existing method is there may lead to leakage of user's public key and secret key in the case of compromised users in the SET-IBS protocol and SET-IBOOS protocol is only efficient for the devices with high computational power. So, in order to overcome this problem an innovative technique is introduced which is called Enhanced Secure Data Transmission protocol which is used to

improve the SE - IBS and SET - IBOOS protocol. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity. Also, to confuse the attackers, encapsulation algorithm is used. In this process, the two cipher texts are used: one is valid cipher text and another one is invalid cipher text. These cipher texts are encapsulated with the corresponding author's encapsulated key. In order to improve the efficiency in the SET-IBOOS protocol, the improved SET-BOOS protocol is proposed in which the online/offline attribute based encryption method is used. An experimental result shows that proposed method achieves high efficiency and high security

[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; The past few years have witnessed increased interest in the potential use of wireless sensor networks (WSNs) in applications such as disaster management, combat field reconnaissance, border protection and security surveillance. Sensors in these applications are expected to be remotely deployed in large numbers and to operate autonomously in unattended environments. To support scalability, nodes are often grouped into disjoint and mostly non-overlapping clusters. In this paper, we present a taxonomy and general classification of published clustering schemes. We survey different clustering algorithms for WSNs; highlighting their objectives, features, complexity, etc. We also compare of these clustering algorithms based on metrics such as convergence rate, cluster stability, cluster overlapping, location- awareness and support for node mobility.

[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;Networking together hundreds or thousands of cheap micro sensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. We develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. Our results show that LEACH can improve system lifetime by an order of magnitude compared with general-purpose multichip approaches.

[5]. K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks,".

[6]L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Key management in wireless sensor network is a complex task due to its nature of environment. Wireless sensor network comprise of large number of sensor nodes with different hardware abilities and functions. Due to the limited memory resources and energy constraints, complex security algorithms cannot be used in sensor networks. Therefore, an energy efficient key management scheme is necessary to mitigate the security risks. In this paper, we present

an Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Network (ESKMS). The proposed technique distributes the keys within a cluster efficiently and updates the pre-deployed keys to mitigate the node compromise attack. We also provide a detailed security analysis of our ESKMS protocol and show its advantages in avoiding different type of attacks from malicious nodes. Finally, using NS-2 simulator, the results shows that ESKMS is more energy efficient and provides a longer network lifetime compared to the existing key management schemes.

[7] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," WSNs usually deployed in the targeted area to monitor or sense the environment and depending upon the application sensor node transmit the data to the base station. To relay the data intermediate nodes communicate together, select appropriate routing path and transmit data towards the base station. Routing path selection depends on the routing protocol of the network. Base station should receive unaltered and fresh data. To fulfill this requirement, routing protocol should be energy-efficient and secure. Hierarchical or cluster-base routing protocol for WSNs is the most energy-efficient among other routing protocols. In this paper, we study different hierarchical routing technique for WSNs. Further we analyze and compare secure hierarchical routing protocols based on various criteria.

[8] W. Diffie and M. Hellman, "New Directions in Cryptography," Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

[9] D.W. Carman, "New Directions in Sensor Network Key Management," Secure data transmission network is a decisive issue for wireless technology networks (WTNs). Clustering is an effective and practical way to enhance the system performance & methods of WTNs.

[10] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," Vehicular ad hoc network (VANET) can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. In this paper, we propose a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, no repudiation, message integrity, and confidentiality. Moreover, we propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication.

The research problem shows the fulfillment and feasibility of our system with respect to the security goals and efficiency.

Problem statement

Secure and Economical data transmission is critical issue in wireless sensor network. In research problem which comes with security

and reduce the energy consumption and computational overhead by using the SET-IBS and SET-IBOOS.

SET-IBS and SET-IBOOS are economical in communication and applying the ID based cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols.

Objectives and Scope

Objectives:

- To present the analysis of different methods based on secure data transmission.
- To design and implement protocol SET-IBS for providing the security as well as solve the orphan node problem.
- To design and implement protocol SET-IBOOS for reducing computational overhead.
- To present the practical analysis of proposed work and its evaluation against the LEACH and Sec LEACH protocol.

Scope:

The scope of this proposed method is efficient and secure design of wireless sensor network. The results aiming in this method are related to security analysis, attack analysis, orphan node problem, energy consumption, computational overhead, etc.

Proposed methodology

In this paper we are presenting the two protocols which is providing the security and efficient data transmission (SET) for wireless sensor networks called as SET-IBS and SET IBOOS, by using the identity based digital signature (IBS) scheme and the identity based online/offline digital signature (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 orphan node 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.

Therefore, in this paper we are improving overall wireless sensor network performance in terms of security as well as better balance of energy consumption than existing protocols.

Comparative Analysis

In order to evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation: Network lifetime, system energy consumption, and the number of alive nodes. For the performance evaluation, we compare the proposed SET-IBS and SET-IBOOS with LEACH protocol [4] and Sec LEACH protocol [8]:

Network lifetime (the time of FND):

We use the most general metric in this paper, the time of first node dies (FND), which indicates the duration that the sensor network is fully functional [1]. Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.

The number of alive nodes:

The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.

Total system energy consumption:

It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols.

In the network simulation experiments, 300 nodes are randomly distributed in a 200m area, with a fixed BS located near part of the area. All the sensor nodes periodically sense events and transmit the data packet to the BS. We assume that the sensor CPU is a low-power high-performance Pentium IV processer of 2.6 GHz, which has been widely used in many sensor products, for example, Crossbow Stargate.

We assume that the BS has unlimited energy. For clustering, we properly set the desired percentage of CH nodes ¼ 10% during one round. In addition, on simulating the SecLEACH protocol, we choose a security level sl ¼ 0:98 for a fixed length of a key ring m ¼ 100. Thus, the probability that two nodes will share a key is Ps ¼ 0:87, which is also referred to as the expected orphan rate of the orphan node problem.

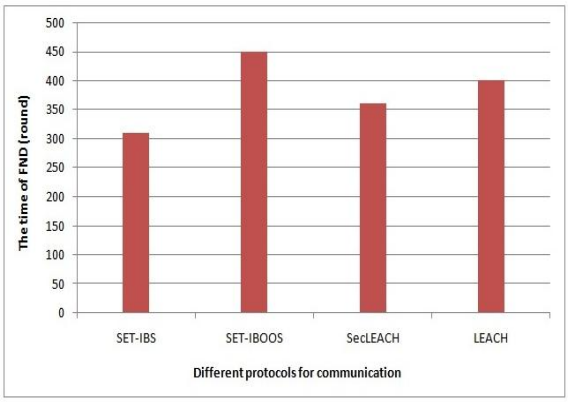

Fig. 1

Fig. 1 illustrates the time of FND using different protocols. We apply confidence intervals to the simulation results, and a certain percentage (confidence level) is set to90 percent.

Fig. shows the comparison of system lifetime using SET-IBS and SET-IBOOS versus LEACH protocol and SecLEACH protocol. The simulation results demonstrate that the system lifetime of SET-IBOOS is longer than that of SET-IBS and SecLEACH protocol.

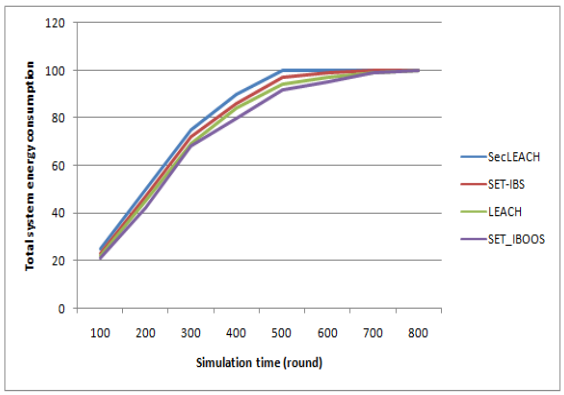

Fig. 2

Fig. 2 illustrates the energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network.

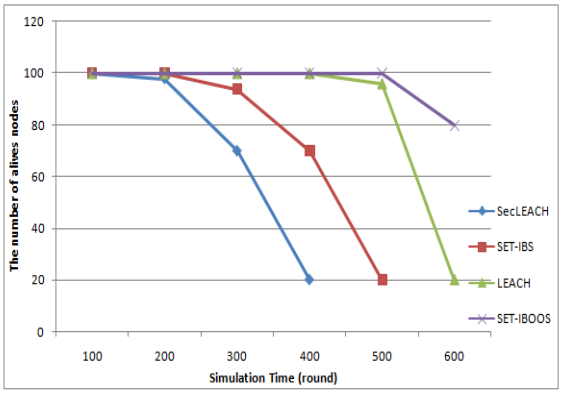

Fig. 3

Fig. 3 shows the comparison of alive nodes' number, in which the proposed SET-IBS and SET-IBOOS protocols versus LEACH and SecLEACH protocols. The results demonstrate that the proposed SET-

IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process. However, the proposed SET-IBOOS has a better balance of energy consumption than that of SecLEACH protocol.

Conclusion

The Protocols like LEACH which are cluster based data transmission protocols suffer from variety of security threats. Adding security to such protocols is little bit tricky since they arbitrarily, occasionally and vigorously rearrange the network's clusters and data links thereby threatening the security and vulnerability of the CWSNs. To overcome the drawback of orphan node problem which is experienced by LEACH, we use the two methods of Identity Based Digital Signature namely the SET-IBS and SET-IBOOS, thus providing efficiency as well as security in the transmission of data among nodes in CWSNs. The efficiency of data transmission increases with respect to both communication and computation cost.

Future work can be done by using the experimental setup by using different number of sensor nodes and with different security attacks. Real time implementation of the system. We can add our concept in real time secure data transmission against different security attacks.

References

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Data 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] 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.

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

[7] 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.

[8] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Data Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[9] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.

[10] 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.

[11] 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.

[12] 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

[13] 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.and Mobile Computing (WiCOM), pp. 1-5, 2008

[14] 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.