IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

Secure and Proficient Information Transmission for group of cluster using Wireless Sensor Networks

[1] K.Kishore kumar [2] N.Phani Kumar,

[1] M. Tech Student , SV College of Engineering, Tirupathi, Andhra Pradesh, India , Email- kishore.kaisetty@yahoo.com.
[2] Asst. Professor SV College of Engineering Tirupathi, Andhra Pradesh, India , Email- phani.n@svcolleges.edu.in

ABSTRACT

Secure information transmission is a basic issue for remote sensor systems (WSNs). Bunching is a successful and pragmatic approach to improve the framework execution of WSNs. In this paper, we concentrate on a protected information transmission for bunch based WSNs (CWSNs), where the groups are framed powerfully and occasionally. We propose two Secure and Effective information Transmission (SET) conventions for CWSNs, called SET-IBS and SET-IBOOS, by utilizing the Personality Based advanced Mark (IBS) plan and the Character Based Online/Disconnected from the net computerized Mark (IBOOS) plan, separately. In SET-IBS, security depends on the hardness of the Diffie-Hellman issue in the matching area. SET-IBOOS further diminishes the computational overhead for convention security, which is critical for WSNs, while its security depends on the hardness of the discrete logarithm issue. We demonstrate the achievability of the SET-IBS and SET-IBOOS conventions as for the security prerequisites and security investigation against different assaults. The counts and reproductions are given to show the effectiveness of the proposed conventions. The outcomes demonstrate that, the proposed conventions have preferred execution over the current secure conventions for WSNs, as far as security overhead and vitality utilization.

INTRODUCTION

Proficient and seclude data communication WIRELESS 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]. 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]. Efficient data communication is one of the most important thing for WSNs. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

Environment And Enthusiasm:

Network-based data Networks in WSNs, has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In a -based WSN (CWSN), every Network has a leader sensor node, regarded as Network-head (CH). A CH aggregates the data collected by the leaf nodes (non- CH sensor nodes) in its Network, and sends the aggregation to the base station (BS). The LEACH (Low-Energy Adaptive Networking Hierarchy) protocol presented by Heinzelman*et al*. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH. In this paper, for convenience, we call this sort of Network-based protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the Network-based architecture in the real world is rather complicated.

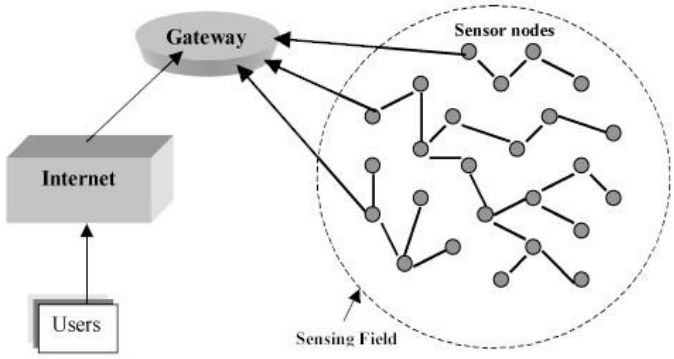
Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's Networks and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH and RLEACH . Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem. This

ISSN 2348 – 7968

problem occurs when a node does not share a pairwise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any Network, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining a CH, when the number of alive nodes owning pairwise keys decreases after a long term operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pair wise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the difficulty of factoring integers from Identity- Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security. Carman first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years, e.g.. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. The IBOOS scheme could be effective for the key management in WSNs. Specifically, the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication. Some IBOOS schemes are designed for WSNs afterwards, such as and this system. The offline signature in these schemes, however, is pre-computed by a third party and lacks reusability, thus they are not suitable for CWSNs.

Architecture of WSN:



Proposed Method:

We propose two Secure and Efficient data Transmission protocols are called SET-IBS and SET-IBOOS.The main idea of both SET-IBS and SET-IBOOS is to authenticate the secured data, by applying digital signatures to data packets, which are ensure in communication and applying the key management for protection. The Secure communication in SET-IBS relies on the ID based process, user public keys are their separate particular identity. Thus, users can obtain the corresponding private keys without auxiliary information passing,its good for communication and saves energy. Identity Based Signature: To provide the security for nodes in the network through the identity based signature only to identify the node authorization in network. Identity based signature node only authorized node to form the cluster and other nodes not allowed to do the any process like information passing, cluster formation in the network. identity Based Online/Offline digital Signature: To enhance the security for data's in the network through the identity based online/offline signature to encrypt the data and send to cluster head in network. most ever Identity based online/offline signature used to encrypt the data between cluster member and cluster head in the network.

Received Signal Strength (RSS) is a readily available and cost-effective method of location estimation, or localization, in wireless sensor networks (WSNs). However, RSS-derived distance estimates are known to be inaccurate, leading many researchers to conclude that RSS is an unreliable method for localization. Based on RSS values of every node in cluster can choose the high receiving power node as choose the cluster head. To receive the RSS value of every node in network and choose the effective clustering and also choose high energy

value node as a cluster head and start the information transferring. The process is achieve energy efficient data transmission in wireless sensor network.

RELATED WORK:

L. B. Jivanadham*et al.* proposed creation of a Secured Cluster-based architecture for a Dynamic Wireless Sensor Network that applies two topology management procedures: node-move-in and node-move-out. The planned security protocol incorporate one round Zero Knowledge Proof and AES algorithm to relate for node authentication, wherever only authenticated nodes will be acknowledged through node-move-in operation. In addition they explained that, it needs $O(h+q)$ rounds for a node to connect into a network securely, where h is the height of the dynamic cluster-based wireless sensor network and q is the number of adjacent nodes of a joining node. After the $O(h+q)$ attempts to join the network, the node is considered as insecure and is eventually discarded from joining the network as in [1].

HichemSedjelmaci*et.al* proposed an intrusion detection framework for a cluster-based WSN (CWSN) that intend to merge the advantage of anomaly and signature detection which are high discovery rate and low false positive, correspondingly. Wireless sensor networks (WSNs) have a enormous potential to be used in vital circumstances like armed forces and commercial applications. On the other hand, these applications are mostly frequently to be deployed in hostile surroundings, where nodes and communication are smart targets to intruders. This makes WSNs susceptible to a range of possible attacks. Because of their characteristics, conservative security methods are not appropriate. So here the authors have proposed an intrusion detection framework for a cluster-based WSN (CWSN) that aims to mergethe advantage of signature detection and anomaly which are high detection rate and low false positive, correspondingly as in [2].

MaanYounis Abdullah *et al* in inspected the problem of security addition to cluster based communication protocols for homogeneous wireless sensor networks containing sensor nodes with very limited resources, and proposed a security resolution where clusters are created periodically and dynamically. Their explanation depicts re-keying function protocol for wireless sensor networks security. They have projected the local administrative functions as master function, derivation function and rekeying function is imprinted with sensor node. A security and performance study proved that it is very proficient in communication, storage, computation and this technique is very successful in defending against a lot of complicated attacks [3]

Tingyao Jiang *et.al* presented a new dynamic intrusion detection method for cluster-based wireless sensor networks(CWSN). The nodes in a wireless sensor network are assembled into clusters depending on the particular relationship swith a cluster head (CH) in every cluster. The projected scheme initially makes use of a clustering algorithm to construct a model of standard traffic behavior, and then uses this model of standard traffic to detect anomalous traffic patterns. Along with the diverse network conditions of clusters, this method might also dynamically set differentdetection factors for different clusters to accomplish a more proper detection algorithm. The performance study

Showed that the projected intrusion detection method can progress the detection accuracy and decrease the false positive rate, and is extremely efficient of the energy preservation as in [4]. Nikolaos A. Pantazis*et.al* presented a classification of energy efficient routing protocols and expanded the classification initially done by Al-Kariki to better describe which issues/operations in each protocol illustrate/enhancethe energy efficiency issues. The distributed behavior and dynamic topology of Wireless Sensor Networks (WSNs)brings in many unusual requirements in routing protocols that should be fulfilled. The main important aspect of a routing protocol, so as to be efficient for WSNs, is the energy usage and the extension of the network's life span. During the past few years, a lot of energy efficient routing protocols have been projected for WSNs. The authors here presented the four types of schemes of energy efficient routing protocols: Network Structure, Communication Model, Topology Based and Reliable Routing. The routing protocols which belong to the first type can be additionally classified as hierarchical or flat. The routing protocols belonging to the second type can be additionally classified as Query-based or Coherent and non-coherent based or Negotiation-based. The routing protocols belonging to the third type can be additionally classified as Location-based or Mobile Agent-based. The routing protocols belonging to the fourth type can be additionally classified as QoS-based or Multipath based. Lastly, a systematic review on energy efficient routing protocols for WSNs is provided as in [5].

Key management methods, except many of them were planned for flat wireless sensor networks, which are not suitablefor cluster-based wireless sensor networks (like LEACH). Here Kun Zhang *et.al* investigated adding security to cluster based

ISSN 2348 – 7968

routing protocols for wireless sensor networks which consist of sensor

nodes with very inadequate resources, and have proposed a security solution for LEACH which is a protocol in which the clusters are created periodically and dynamically. The solution proposed by authors makes use of enhanced Random Pair-wise Keys (RPK) method, an optimized security method that depends on symmetric key methods and is a lightweight and conserves the heart of the original LEACH protocol. Simulations demonstrate that security of RLEACH has been enhanced, with reduction in energy utilization and very less operating cost as in [6].

In Wireless Sensor Networks (WSNs), a crucial security necessity is authentication to evade attacks against secure Communication, and to diminish DoS attacks utilize the limited resources of sensor nodes. Resource restraint of sensornodes are major difficulty in applying strong public key cryptographic based mechanisms in WSNs. To deal with theproblem of authentication in WSNs, Yasmin, R *et.al* have proposed secure and efficient framework for authenticatedbroadcast/multicast by sensor nodes and for outside user authentication, which uses identity based cryptography and online/offline signature schemes. The most important objectives of this framework are to allow all sensor nodes in the network, initially, to broadcast and/or multicast an authenticated message rapidly; secondly, to confirm the broadcast/multicast message sender and the message contents; and lastly, to confirm the authenticity of an outside user.The projected framework is also evaluated by means of the most secure and efficient identity-based signature (IBS)schemes as in [7].

A secure routing for cluster-based sensor networks is where clusters are formed periodically and dynamically. Together with the investigation of ID-based cryptography for security in WSNs, Huang Lu *et.al* proposed anew secure routing protocol with ID-based signature scheme for cluster-based WSNs within which the security is dependent on the hardness of the Diffie-Hellman problem in the random oracle model. Here the deficiency inthe secure routing protocols with symmetric key pairing is pointed out by authors. Because of the communication operating cost for security, authors provide simulation investigation results in details to demonstrate how various parameters act among energy efficiency and security as in [8].

A process by which data is collected and sent from sensor nodes to the base station is known as data aggregation. It is completed via some sensor nodes called aggregators. A key role is played by security in data aggregation procedure to make sure confidentiality and privacy of aggregated data., In [9] Nguyen Xuan Quy et.al proposed a data aggregation method for cluster-based WSN that improves the security against attackers. This method was based on accelerated homomorphism public key encryption which presents continuous suppression of and supports hop-to-hop verification. The logical investigation and association demonstrate that this approach has both lower computational and better security performance as compared to other approaches as in [9].

SYSTEM DESCRIPTION AND PROTOCOL

This sector explained the network architecture, security vulnerabilities, and protocol themes.. Network Architecture Consider a CWSN consisting of a fixed BS,AODV and a large number of wireless elements .

The BS is a trusted authority (TA).Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodesare grouped into clusters, and each cluster has a CH sensornode, which is elected autonomously. Leaf (non-CH) sensornodes join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy. In addition, we assume that all sensor nodes and the BS aretime synchronized

with symmetric radio channels, nodesare distributed randomly, and their energy is constrained. The CWSNs in data sensing, processing, and transmission consume energy of sensor elements. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node(e.g., a CH) aggregates data and sends it to the BS is preferred than the method that each sensor node directly sends data to the BS [1], [3]. A sensor node switches into sleep mode for energy saving when it does not sense ortransmit data, depending on the time-division multiple access (TDMA) control used for data transmission. In thispaper, the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs above. These are all the sensors networks are used to routing protocols used by transmitted by the signal through wireless networks signals transferred by the data using protocols. The AODV protocol message exchanges of the AODV protocol. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello

messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination to the routing protocol process through sensor networks.

Security liabilities and Protocol purpose:

The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2], [23]. Especially attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs fundamentally. If an attack emanages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other handan attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogu information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by round swhich makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it hardefor an adversary to identify and compromise important nodes (i.e., CH nodes).

CONCLUSION:

In this paper, we first reviewed The Proficient And Seclude Data Communication On Network Based Networks through 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,AODV and SET-IBOOS protocols are efficient in communication and applying the ID-based crypto-system, 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 and these are in the used NS2 TOOL for see the result of this paper .using linux operating system.

REFERENCES:

The base paper referred to‖ Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks‖ Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE.

[2] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] K. Pradeepa, W.R. Anne, and S. Duraisamy, ―Design

ISSN 2348 – 7968

[9] Implementation Issues of Clustering in Wireless Sensor Networks,‖ Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28,2012.

[10] L.B. Oliveira et al., ―SecLEACH-On the Security of Clustered Sensor Networks,‖ Signal Processing, vol. 87, pp. 2882-2895, 2007. [11]. 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.