ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

A Review on Efficient and Secure Transmission of data for Cluster-Based Wireless Sensor Networks

Malhar Bhandari[1], Sulabha Patil[2], T. Raju[3]

P.G. Student, Dept of M.Tech C.S.E/W.C.C, A.G.P.C.E, Nagpur, Maharashtra, India [1]

Assistant Professor, Dept of M.Tech C.S.E/W.C.C, A.G.P.C.E, Nagpur, Maharashtra, India [2]

Assistant Professor, Dept of M.Tech C.S.E/W.C.C, A.G.P.C.E, Nagpur, Maharashtra, India [3]

Abstract: In the past few years secure transmission of data along with efficiency is a critical issue for wireless sensor networks (WSNs). Clustering is an effectual and convenient way to enhance performance of the WSNs system. In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and sporadically. We make use of two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by means of the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, correspondingly. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing area. SET-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defence depends on the stability of the problem of discrete logarithm.

Keywords: CWSN, Cluster-Head, node, SET

I. 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 issues 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 many 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, known as cluster-head (CH). A CH collects the data gathered by the leaf nodes (non- CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security. Digital signature is one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity- Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number or its name. This states that security must encompass every phase of the design of a wireless sensor network application that will require a high intensity of security. Probable applications comprise monitoring isolated or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental supervision. A primary topic that must be addressed when using cluster-based security protocols based on symmetric session keys is the means used for ascertaining the session keys in the primary place. A vital design concern for security protocols based on

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

symmetric keys is the degree of session key among the nodes in the system. On the other hand, it has the clear security drawback that the negotiation of a single node will disclose the global key.

II. BACKGROUND

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].

Hichem Sedjelmaci *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 merge the advantage of signature detection and anomaly which are high detection rate and low false positive, correspondingly as in [2].

Maan Younis 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 (LAFs) 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 as in [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 relationships with 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 different detection 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/enhance the 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].

Wireless sensor networks routing protocols the entire time ignore security problem at the scheming step, as plenty of explanation of this problem are available, using key management is one of them. Researchers have projected several

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

key management methods, except many of them were planned for flat wireless sensor networks, which are not suitable for cluster-based wireless sensor networks (like LEACH). Here Kun Zhang *et.al* investigated adding security to cluster-based 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 sensor nodes are major difficulty in applying strong public key cryptographic based mechanisms in WSNs. To deal with the problem of authentication in WSNs, Yasmin, R *et.al* have proposed secure and efficient framework for authenticated broadcast/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 a new 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 in the 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].

Current day progress in Wireless Sensor Networks makes them very important to apply in number of practical applications. Hence, security concerns are more noteworthy in WSNs. WSNs are prone to various types of attacks since they contain tiny and cheap devices and are installed in unprotected and open surroundings. Yan, K.Q *et.al* proposed an Intrusion Detection System (IDS) created in cluster head. The IDS projected is a Hybrid Intrusion Detection System (HIDS). It contains misuse and anomaly recognition component. The objective is to increase the detection rate and lower the false positive rate by the benefits of misuse and anomaly detection. On the other hand, to incorporate the detect results and to report the types of attacks is done by the means of an administrative module as in [10].

III. **THE PROBLEM**

A. Network Design

Let us consider a CWSN consisting of a preset base station (BS) and a big number of wireless sensor nodes, which are uniform in functionalities and capabilities. We presume that the BS is always consistent, i.e., the BS is a trusted entity. In the meantime, the sensor nodes may be negotiated by external attackers, and the transmission of data may be interrupted from assault on wireless channel. In a CWSN, sensor nodes are assembled into clusters, and every cluster has a cluster-head (CH) sensor node, which is chosen separately. Leaf sensor nodes which are non-CH nodes connect a cluster depending on the receiving signal power and transmit the sensed data to the BS through CHs to conserve system energy. The CHs executes data synthesis, and transmit data to the BS straight away with reasonably high energy. Also,

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

we presume that, all sensor nodes and the BS are time coordinated with symmetric radio channels, nodes are disseminated arbitrarily, and their energy is controlled.
During data sensing, processing and communication in CWSNs, energy of sensor nodes is consumed. The charge of data transmission is lot more costly than that of data processing. Thus, the technique that the intermediary node (i.e. a CH) collects data and sends it to the BS is favored, than the technique that every sensor node directly sends data to the BS. A sensor node change into sleep mode for power saving while it does not sense or transmit data and it depends on the TDMA (time division multiple access) control used for data transmission. In this paper, the used protocols SET-IBS and SET-IBOOS are both planned for the same CWSNs situation.

B. Security Threats and Protocol Goals

The cluster based protocols (like LEACH) which are the data transmission protocols for WSNs, are susceptible to many security attacks. In general, the attacks to Cluster Heads in CWSNs can produce serious damage to the network, since data aggregation and data transmission rely on the CHs primarily. If an invader manages to act as if it's a CH or negotiate the CH, it can incite attacks such as selective forwarding attacks and sinkhole, thus upsetting the network. Alternatively an attacker may mean to insert false sensing data into the WSN, like pretending as a leaf node transferring false information to the CHs. However, LEACH like protocols are extra tough against insider attacks rather than other types of protocols in WSNs. Since CHs are rotating from nodes to nodes in the network by rounds making it harder for intruders to recognize the routing fundamentals as the intermediary nodes and assault them. The properties in LEACH-like protocols decrease the threat of being attacked on intermediary nodes, and make it difficult for an attacker to discover and compromise essential nodes. The aim of the planned secure transmission of data for CWSNs is to assure a protected and a well-organized transmission of data between CHs and leaf nodes, with transmission between BS and CHs. Most of the present protocols used for secure transmission of data undergo he orphan node problem. We intend to solve this orphan node problem in this paper by means of the crypto-system based on ID that gives the warranty of security requirements, and use SET-IBS by using the Identity-Based digital Signature scheme. Besides, SET-IBOOS is also used to decrease the computational operating cost in SET-IBS with the IBOOS method.

IV. **IBS and IBOOS INTENDED for CWSNs**

In this part, we introduce the IBS method and IBOOS method used in the paper. Here we can see that the usual schemes are not specially intended for CWSNs. Therefore we adjust the usual IBS method for CWSNs by allocating functions to different types of sensor nodes, based on [11]. Now for extra reduction in the operation cost in authentication and the signing procedure of the IBS method, we adjust the usual IBOOS scheme for CWSNs, based on [12].

A. IBS Method Intended for CWSNs

An IBS method applied for CWSNs consists of the following four processes:

- *Setup at the BS*: The BS creates a master key *msk* and public parameters *param* for the private key generator (PKG), and provides these to every sensor nodes in network.
- *Key extraction*: Given an ID string, a sensor node creates a private key sek_{ID} related with the ID by means of *msk*.
- *Signing of signature*: Given a time-stamp t, signing key θ and message M, a signature SIG is created by the sending node.
- *Verification of the data receiving nodes:* Given the SIG, ID and M, the receiving node yields "accept" if *SIG* is legal, and outputs "reject" if not.

The complete explanation of the original IBS scheme is given in [11]

B. IBOOS Method Intended for CWSNs

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

An IBOOS scheme implemented for CWSNs consists of following five processes:

- *Setup at BS:* Similar to that of the IBS method.
- *Extraction:* Similar to that of the IBS method.
- *Offline signing at the CHs:* Given time-stamp t and public parameters, the CH sensor node creates an offline signature $SIG_{offline}$, and sends out to the leaf nodes in its cluster.
- *Online signing online signing of the data sending nodes:* From the private key sek_{ID}, message M and $SIG_{offline}$, a sending node (leaf node) creates an online signature SIG_{online}.
- *Verification of the receiving nodes:* Given $SIG_{online,}$ ID and M, the receiving node (CH node) yields "accept" if SIG_{online} is legal, and yields "reject" if not.

The complete explanation of the original IBS scheme is given in [12]

V. 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 intend to 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. We intend to increase the efficiency with respect to both communication and computation cost.

REFERENCES

[1] Jivanadham, L.B, Islam, A.K.M.M., Mansoor, N., Baharun,"A Secured Dynamic Cluster-Based Wireless Sensor Network", 2012 Fourth International Conference, Publication Year, Page(s): 223- 228, 2012

[2] Sedjelmaci, H.; Senouci, S.M.; Feham," Intrusion detection framework of cluster-based wireless sensor network", M. Computers and Communications (ISCC), 2012 IEEE Symposium Publication, Page(s): 857- 861, Year: 2012

[3] Abdullah, M.Y., Gui Wei Hua," Cluster-Based Security for Wireless Sensor Networks", Communications and Mobile Computing, CMC '09. WRI International Conference on Volume: 3, Page(s): 555- 559, Publication Year: 2009

[4] Tingyao Jiang, Gangliang Wang, Heng Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks", World Automation Congress (WAC), Page(s): 259- 261, Publication Year: 2012

[5] Nikolaos A. Pantazis, Stefanos A.Nikolidakis, Dimitrios D.Vergados,"Energy-Efficient Routing Protocols in Wireless Sensor Networks", A Survey IEEE Communications surveys & tutorials, vol. 15, no. 2, second quarter 2013

[6] Kun Zhang, Cong Wang, Cuirong Wang, "Wireless Communications, Networking and Mobile Computing", 2008, WiCOM 2008. 4th International Conference, Page(s): 1- 5, Publication Year: 2008

[7] Yasmin, R., Ritter, E.;" An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures", Guilin Wang Computer and Information Technology (CIT), 2010 IEEE 10th International Conference, Page(s): 882- 889, Publication Year: 2010

[8] Huang Lu, Jie Li, Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature" in H. Global Telecommunications Conference (GLOBECOM 2010), Page(s): 1- 5, Publication Year: 2010

[9] Nguyen Xuan Quy, Mingi Kyun, Dugki Min,"Security-enhanced energy-efficient data aggregation for cluster-based wireless sensor networks", Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference, Page(s): 1- 5, Publication Year: 2008

[10] Yan, K.Q., Wang, S.C., Wang, S.S., Liu, C.W, "Hybrid Intrusion Detection System for enhancing the security of a cluster-based Wireless Sensor Network Yan," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Volume:1, , Page(s): 114- 118, Publication Year: 2010

[11] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in Lecture Notes. Computer Science, - SAC, 2003.

[12] J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme," in Lecture Notes. Computer Science, - Appl. Cryptography Network Security, 2009.