ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Enhanced Multi Clustered Security System For Wireless Sensor Network

R.Sushma
M.Tech Student,
Department of Computer Science and Engineering,
MVSR Engineering College,Hyderabad, India

Md.Abdul Azeem
Associate Professor,
Department of Computer Science and Engineering,
MVSR Engineering College,Hyderabad, India

Abstract:

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two secure and efficient data transmission (SET) protocols for CWSNs, 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. it has been proposed in order to reduce the computation and storage cost to authenticate the encrypted sensed data by applying digital signature to message packet which are efficient in communication and applying key management for security. The pairing parameters are distributed and preloaded in all sensor nodes by base station initially.

Keywords:

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

INTRODUCTION:

Wireless Sensor Networks (WSNs) can provide low cost solutions to various real world problems. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme[1], 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.

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 protocolsfor efficiency by calculations and simulations, respectively, with respect to both computation and communication. The data transmission protocols for WSNs, including cluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks. 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 attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

On the other hand, an attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogus information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs. It is because CHs are rotating from nodes to nodes in the network by rounds, which 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 harder for an adversary to identify and compromise important nodes (i.e., CH nodes).

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secures transmission protocols for CWSNs in the literature however, apply the symmetric key management for security, which suffers from the orphan node problem . In this paper, we aim to solve this orphan node problem by using the ID-based cryptosystem that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational over-head in SET-IBS with the IBOOS scheme [6].

1.RELATED WORK:

The paper[2] author proposed an Adaptive Staggered SLEEP Protocol (ASLEEP) for efficient power management in wireless sensor networks targeted to periodic data acquisition. This protocol dynamically adjusts the sleep schedules of nodes to match the network demands, even in time-varying operating conditions. It uses the CSMA scheme for process the data, but it may be not efficient in fixed WSN network and there is no detail to data management.

The paper[3] author present a cluster based routing algorithm. One of author's main goals is to design the energy efficient routing protocol. This algorithm makes the best use of node with low number of cluster head know as super node. Here author divided the full region in equal zones and the center area of the region is used to select for super node. Each zone is considered separately and the zone may be or not divided further that's depending upon the density of nodes in that zone and capability of the super node.

In this paper author considered, cluster head changes when the cluster head is failed. It may be the problem to sensing in that area.The paper [4]author investigate the usefulness of enforcing a minimum separation distance between cluster heads in a cluster based sensor network, thereby prolonging network lifetime by spreading the cluster heads, thus lowering the average communication energy consumption.the minimum separation distance between cluster heads in a cluster based sensor network, thereby prolonging network lifetime by spreading the cluster heads and it shows that our sensor network performs up to 150% better when introducing a minimum separation distance between cluster heads, comparing the number of messages received at the base station, the author consider only about the distance between the cluster heads to improve network lifetime but not energy levels.

2.PROPOSED SCHEME:

When sensor nodes are static in nature, Initially at the time of deployment all node possess unique ID, a certificate (signed by authority i.e. base station), a unique shared key (shared with base station) and a public key of the base station. The certificate is used to authenticate any node at the time of neighbor detection with the public key of the base station; unique shared key is used to communicate with the base station through the lifetime of the network. Network is break by hierarchical approach in to clustered layers. Cluster is a group of nodes with one cluster head (CH).Cluster head responsible for the routing from the cluster to different cluster heads or base station. The process of traveling data is lower clustered layer to higher one. Several techniques are used in current clustering algorithms to achieve longer life time [5]. CH rotation: CH rotation between sensors is necessary because CHs consume more energy than the normal sensors due to their responsibilities of data gathering from sensors and data transmission to the Base Station.

Energy aware CH election: In cluster the node is elected as CH which has high residual energy to even the power usage.Cluster size: Big cluster's CH consumes more energy than small cluster's CH. Cluster size is also mattered in energy management.Most popular energy efficient hierarchical clustering protocols are LEACH (Low Energy Adaptive Clustering Hierarchy):it is routing protocol in which the data is delivered to the base station using cluster based approach. In LEACH, cluster heads selected randomly.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The selection of Cluster head depends on decision made 0 and 1. If the number is less than a threshold, the node, becomes a cluster head for the current round. The threshold is set[14].

$$T(n)= \begin{cases} \dfrac{p}{1-p*(r*\mathrm{mod}1/p)} & \text{if } n \in G \\ 0 & \text{else} \end{cases}$$

Where p is the desired percentage of cluster head, r is the current round. G is the set of nodes that have not been cluster head in the last 1/p rounds.This algorithm is simple but does not guarantee about even distribution of cluster heads over the network [19].In multi cluster security system are using Elliptic Curve Cryptography (ECC) is known to provide equivalent level of security with lower number of bits used. Reduced bit usage implies less power and logic area are required to implement this cryptographic scheme. This is particularly important in wireless networks, where a high level of security is required, but with low power consumption. The equation of an elliptic curve is given as[8],

$$Y2 = X3 + aX + b$$

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. The key part of the process is that Alice And Bob exchange their secret key in a mix only. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data. For generation of a shared secret key between A and B using ECDH, both have to agree up on EC domain parameters. Both end have a key pair consisting of a private key d(randomly selected integer less then n, where n is the order of the curve) and another is a public key Q= d*G (G is the generator point). Let (dA, QA) be the private-public key pair of A and (dB, QB) be the private-public key of B.

1. The end A Computes KA= (XA, YA) = dA * QB
2. The end B Computes KB= (XB, YB) = dB * QA
3. Since dA * QB = dAdB G= dBdA G = dB * QA . Therefore KA= KB and hence XA =XB
4. (Where G is generator point)
5. Hence the shared secret is KA.

Since it is practically impossible to find the private key dA or dB from the public key KA

3.SIMULATION AND RESULTS:

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.34.

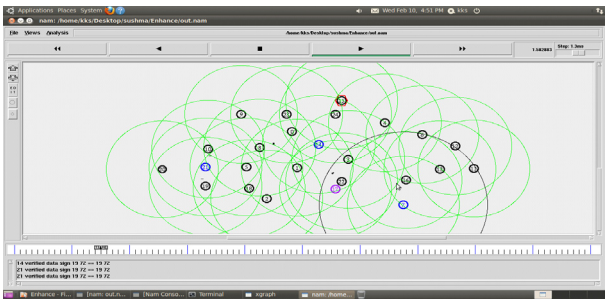


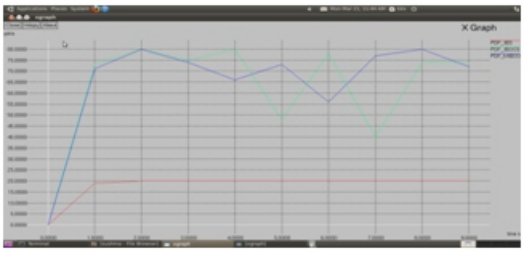
Figure 3.1 Node Verification In figure 3.1 shows the nam output of verification i.e., identifying the authenticated nodes.

Results :

No of nodes	IBS malicious	IBOOS	Hierachical Cluster based
25	21.52 %	21.25 %	47.98 %
100	24.6 %	24.8%	55.8 %
200	28.5 %	28.4%	65.90 %

Table 1: Energy levels for Packet Delivery of hello.

The above table describe the energy level of the packets of hello message for different nodes .



In figure 3.2 shows packet delivery. From above figure we can see the Xgraph for the analysis of Energy levels in Cluster IBS mali, Security SET-IBOOS, Hierarchical Cluster based IBOOS. X-axis consists of time in seconds and Y-axis consists of packets.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

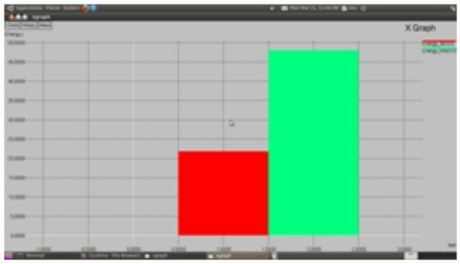


Fig 5.5: The Energy levels of SET-IBOOS, Hierarchical Cluster based IBOOS From above figure we can see the Xgraph for the analysis of the IBOOS consisting of Energy level 22% and MIBOOS consisting of Energy level is 46%. X-axis consists of time in seconds and Y-axis consists of Energy.

4.CONCLUSIONS:

The Security and Data Transmission in Cluster founded Wireless Sensor Networks. The Offered SET-IBS and SET-IBOOS to protect and effective transmission protocols, respectively for Cluster founded Wireless Sensor systems. SET-IBS and SETIBOOS are produced in connection and applying the ID based crypto-system, which accomplishes security in multi cluster security system, as well as clarified the orphan node difficulty in the protected transmission protocols with the symmetric key management, using SET-IBOOS and SET-IBS are less auxiliary security overhead is preferential for secure data transmission. Future advancement shows the energy consumption for every node in the network with the transfer data in secure and efficient for multi cluster security system .

REFERENCES:

1.“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,2014.
2.Giuseppe Anastasi, Marco Conti, Mario Di Francesco, “Extending the Lifetime of Wireless Sensor Networks through Adaptive Sleep”, 2007.
3.Ashim Kumar Ghosh1, Anupam Kumar Bairagi2, Dr. M. Abul Kashem3, Md. Rezwan-ul-Islam1, A J M Asraf Uddin1 “Energy Efficient Zone Division Multihop Hierarchical Clustering Algorithm for Load Balancing in Wireless Sensor Network. ”, 2011.
4.Ewa Hansen, Jonas Neander, Mikael Nolin and Mats Björkman “Energy-Efficient Cluster Formation for Large Sensor Networks using a Minimum Separation Distance”,
5.L Xu, GMP O’Hare, R Collier “A Balanced Energy-Efficient Multihop Clustering Scheme for WSN”- Wireless and Mobile Networking Conference (WMNC), 2014 7 th I FIP DOI: 10.1109 / WMNC .2014. 6878886, IEEE-2014.
6.S. Backtir. “Frequency domain finite field arithmetic for elliptic curve cryptography”. PhD Thesis. Worcester Polytechnic Institute. 2008.
7.B Manzoor, N Javaid, O Rehman, M Akbar, ”Q-LEACH: Anew Routing Protocol for WSNs”- Procedia Computer Science 19 (2013) 926 – 931, Elsevier.
8.Makhamisa Senekane, Sehlabaka Qhoboshean, and B.M. Taele” Elliptic Curve Diffie-Hellman Protocol Implementation Using Picoblaze” IJCSNS , VOL.11(6) , June 2011.
9.Sinem Coleri Ergen and Pravin Varaiya, “TDMA Scheduling Algorithms for Wireless Sensor Networks”, 2009.
10.S. Backtir. “Frequency domain finite field arithmetic for elliptic curve cryptography”. PhD Thesis. Worcester Polytechnic Institute. 2008.
11.Chenyang Lu, Brian M. Blum, Tarek F. Abdelzaher, John A. Stankovic, Tian He, “RAP: A Real-Time Communication Architecture for Large-Scale Wireless Sensor Networks”, 2002.
12.Injong Rhee, Ajit Warrier, Jeongki Min, “DRAND: Distributed Randomized TDMA Scheduling For Wireless Ad-hoc Networks”, Injong Rhee, 2009.
13.Y. Liu, I. Elhanany, and H. Qi, “An energy-efficient QoS-aware media access control protocol for wireless sensor networks,” Nov. 2005.
14.Qing Bian, Yan Zhang,”Research on Clustering Routing Algorithms in Wireless Sensor Networks,” International Conference on Intelligent Computation Technology and Automation in 2010.
15.Sathishkumar.S,Anitha.A,Revathi.S’,”Secure Multi-Hop Data Transmission Over Cluster Based Wireless Sensor Network”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.