International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

REVIEW ARTICLE

ISSN: 2321-7758

APPLY THE RSS METHOD TO INCREASE LIFETIME OF CLUSTER BASED WIRELESS SENSOR NETWORK

VENKATESHWARAN.N[1], Prof SATHEESH KUMAR.D[2]

[1]P.G Student, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamilnadu, India

[2]Assistant Professor, Computer Science and Engineering, Hindusthan College of Engineering and Technology, Tamilnadu, India

Article Received:10/05/2015 | Article Revised on:17/05/2015 | Article Accepted on:22/05/2015

ISSN:2321-7758
International Journal of Engineering Research-Online
A peer-reviewed, open access International scientific journal
www.ijoer.in

ABSTRACT

The two Secure and Efficient data Transmission protocols are called SET-IBS and SET-IBOOS, by using the IBS scheme and the identity based online/offline digital signature scheme, respectively. Both SET-IBS and SET-IBOOS is to authenticate the secured sensed data, by applying digital signatures to message packets. Both the protocols are only concern about the security purpose of the process. In this process apply the RSS (Received Signal Strength) method to increases the lifetime of the whole process. The RSS technique as to choose the effective cluster head as high receiving capabilities in cluster group and based on efficient cluster head to increase the wireless sensor network life time and achieve energy effective wireless sensor network. Keywords – CWSNs, IBOOS, CH,SET,node.RSS

INTRODUCTION:

The wireless sensor networks (WSNs) has grown enormously in recent years, particularly important need as scalable and energy-efficient routing and data gathering and aggregation protocols in corresponding large-scale environments. In most wireless sensor network (WSN) applications nowadays the entire network must have the ability to operate unattended in harsh environments in which pure human access and monitoring cannot be easily scheduled or efficiently managed or it's even not feasible to all the working areas. Energy of the sensors and the possibility of having damaged nodes more populations of sensors are expected, that hundreds or even thousands of sensor nodes will be involved. Cluster based wireless sensor networks have been widely used due to the easily organize the nodes. The cluster formation process eventually leads to a two-level hierarchy where the CH nodes form the higher level and the cluster-member nodes form the bottom level. The each sensor nodes periodically transmit their data to the corresponding CH nodes. The BS is the data processing point for the data received from the sensor nodes, and where the data is accessed by the users. The CH nodes act as bridge between the base station and cluster head. The function of each CH, as already noted, it perform common functions for all the nodes in the cluster process, like this type of the data before sending it to the BS. The BS is the sink for the CHs. Different from previous analysis of network lifetime, analyses the node energy consumption in different regions through the differential analysis method. Thus, the optimal parameters which maximize the lifetime can be obtained and the detailed energy consumption in different regions at different time can be also obtained.

The Identity-Based digital Signature is 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 individuality. This protection must encompass every phase of the design of a wireless sensor network application that will require a high security. Likely applications comprise monitoring isolated locations, object tracking in fighting environments.

II LITERATUR SURVEY

The main focus of the literature survey will be on the analysis of efficient transmission and dealing with network protection. Transmission and protection are separate domains. Improvement in both of these domains have advanced researches. Here our idea is to combine the advantages of both these ideas. In Wireless Sensor Networks (WSNs), mandatory security is authentication to evade attacks against secure processing, and to smaller 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 .In this paper [8]. "Secure Routing in Wireless Sensor Networks "Secure routing in WSN has been a major challenge due to node mobility and resource constraint nature of such networks. That identity-based cryptography can play a vital role in defending against many complex cross-layer attacks on WSN routing protocol and also location and energy aware identity-based cryptographic routing can prevent a selective attacks, causes are Time complexity and It's not fully Secured.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 randomly. Their describe re-keying function protocol for wireless sensor networks protection process. They have monitor the local administrative functions (LAFs) as admin function, hierarchical function and rekeying function is imprinted with sensor node. A security and performance study proved that it is very proficient in transmission, storage, evaluation and this technique is very successful in defending against a lot of complicated attacks as in [3] the complexity in verification of digital signatures in a hierarchical system. Provides a simpler model for key management. With tiny PBC cryptographic use binary elliptical curves over prime curves provides significant offer computational advantages in a resources constraint environment. The problems are proactive routing provides additional overhead due to frequent routing updates. Symmetric key cryptography has major drawbacks with regard to key management and the security is based on pre shared secret keys. Tingyao Jiang et.al presented a new dynamic intrusion detection method for cluster-based wireless sensor networks(CWSN).In a wireless sensor network nodes are assembled into clusters depending on the particular relationships with a cluster head (CH). The process initially makes use of a clustering algorithm to construct a model of standard traffic behaviour, and then uses this model of standard traffic to detect anomalous traffic patterns. Along with the diverse network situation in clusters, this might also randomly set different detection factors for different clusters to accomplish a more proper detection algorithm. An authentication framework for wireless sensor networks using identity-based signature: implementation and evaluation "Integer arithmetic is very efficient for sensor nodes in terms of time and energy consumption. With the help of BNN-IBS as IBOOS does not affect the security process.this process as to compute the offline part before the message is known and store it. IBOOS is very efficient in terms of computation cost for resource constraints. IBOOS is the most efficient scheme for time critical applications of WSNs when compared with existing signature based identification. A arithmetic is very efficient for sensor nodes in terms of time and energy consumption. With the help of BNN-IBS as IBOOS does not affect the protection.It protect to compute the offline part before the message is known and store it. IBOOS is very efficient in terms of computation cost for resource constraints. IBOOS is the most efficient scheme for time critical applications of WSNs when compared with existing signature based authentication schemes.

"Efficient identity-based threshold signature scheme from bilinear pairings in the standard model "Threshold signing protocol is optimal in terms of communication complexity and communication channel requirement. It is also proved with optimal resilience in the standard model. It includes both unforgeability and robustness. Threshold signature scheme increase the availability of the signing agency. The same time to increase the protection against forgery by making it harder for the adversary to learn the secret key.In an energy efficient routing protocols and expanded the classification initially done by Al-Kariki to better describe which enhance the energy efficiency issues. Current day progress in Wireless Sensor Networks makes them very important to apply in number of practical working process. The protective are more mandatory in WSNs.Intrusion Detection System (IDS) created in lard cluster. It contains misuse and anomaly identifying component. This is to increase the detection rate and lower the false positive rate by the benefits of misuse and unusual detection. The another process as, to incorporate the detect results and to report the types of attacks is done by the means of an administrative module.

III. PROPOSED METHODOLOGY

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.

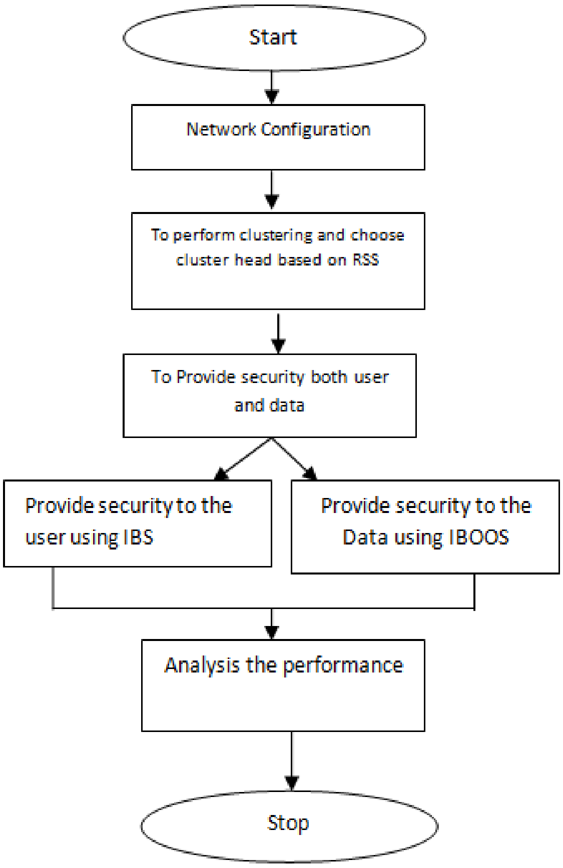
RSS scheme:

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.

Cluster performance:

The cluster performance for choosing efficient cluster head in particular cluster area based on RSS value of each node in network and this process is used for achieving energy efficient data transmission in network.

Data flow Diagram


Start
Network Configuration
To perform clustering and choose cluster head based on RSS
To Provide security both user and data
Provide security to the user using IBS
Provide security to the Data using IBOOS
Analysis the performance
Stop

Comparison analysis:

First the implementation of RSS concept in this system is achieved through implementations in NS2. The existing and proposed system parameters are considered one against the other to see how efficient the enhanced system is when compared to the existing system. These graphs are plotted using XGRAPH and combined together into a single WISH file to show the comparison analysis in NS2.

IV. CONCLUSION

The protocols SET-IBS and SET-IBOOS is to authenticate the secure data, by applying digital signatures to message packets. Increasing the life time of the process by Apply the RSS (Received Signal Strength) method to choose the effective cluster head as high receiving capabilities in cluster group and based on efficient cluster head to increase the wireless sensor network life time and achieve energy effective wireless sensor *network.*

REFERENCES

[1]. 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

[2]. Nikolaos A. Pantazis, Stefano's 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

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

[4]. 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.

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

[6]. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks"Pro.. IEEE Sixth Int'l Symp. Network Computing and Applications(NCA), pp. 145-152, 2007.

[7]. 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.

[8]. Shamir, "Identity-Based Cryptosystems and SignatureSchemes," Proc. Advances in Cryptology (CRYPTO),pp. 47-53, 1985.

[9]. 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.

[10]. A. Shamir, "Identity-Based Cryptosystems and SignatureSchemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.

[11]. R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology(CIT), pp. 882-889, 2010.