International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 17615-17630

http://www.ripublication.com

An Effective Compression Based Secure Authentication Protocol for WSN

[1] Mr. A.S.Anshad, [2] Dr. R.Radhakrishnan
[1] Assistant Professor, Department of ECE, Malabar College of Engineering and Technology, Thrissur, Kerala, India.
[2] The Principal, Vidhya Mandhir Institute of Technology, Erode, Tamilnadu, India

Abstract

Conventional data compression techniques developed for wired and wireless sensor networks are not well suited for applications due to entrust of network management system and high power consumption. In the past, data compression techniques were used to compress the data in network effectively. Most of the systems are unable to identify the original data with improper security. In this research work, we proposed an Effective Compression based Secure Authentication Protocol (ECSAP) for load balancing, data compression and authentication. To achieve this, load balanced multipath routing is established based on popularity of sensor nodes and link stability in random topology. Data compression is achieved by means of information source entropy which includes reference database. Including this, asymmetric encryption and decryption method is also proposed for identifying and isolating the malicious nodes, packet integrity and node authentication in network. This encryption scheme also achieves network reliability and node stability during entire packet transmission phase. Simulation results shows that the ECSAP provides better packet delivery ratio, low end to end delay, more network stability rate and less control overhead than existing schemes.

Keywords: WSN, Load balancing, Multipath Approach, Popularity of sensor nodes, Data Compression, Asymmetric encryption and decryption, Data integrity, Pause time, packet delivery ratio, stability rate and delay etc.

Introduction

A. Wireless Sensor Network

Recent technology development in the fields of wireless communication and MEMS has facilitated the extensive distribution of wireless sensor networks (WSNs) which

are reliable, accurate, flexible, inexpensive and easy to deploy. In many applications, for instance, environment monitoring and battlefield spying, the nodes are vulnerable to be attacked by passive eavesdropping, active intrusion, message flooding, fake information inserting, etc. Among the above hostile attacks, passive eavesdropping helps adversaries intercept private information. Active intrusion makes it possible for adversaries to delete information, insert false information or impersonate nodes, which destroy the usability, integrity, security certificate and non-reputation of WSNs. Unfortunately, the available complicated encryption algorithms are unsuitable for WSNs because of the restricted capabilities of low cost nodes. Hence, the WSNs usually adopt security method based on symmetric cryptographic methods.

However, the intrusion detection and prevention schemes with cryptographic protection are unable to identify the destructive threat by the authenticated nodes which have been compromised. If the compromised nodes cannot be identified in time, secret information may be revealed and the whole network could be under the control of the adversaries. Therefore, an efficient mechanism is urgently needed to identify the compromised nodes and take measures to minimize the destruction or loss in the network.

Data compression is a well-established research area, despite the extraordinary advances in the computational capability of embedded devices,most existing algorithms still cannot be directly ported to wireless sensor nodes because of the limited hardware resources available, particularly program and data memory [1]. Even though many of the time-honored compression algorithms could be executed in modern wireless sensor nodes, they would leave few resources available for the nodes to carry out other tasks such as sensing and communication. More importantly, these nodes would have significantly fewer opportunities to enter deep sleep modes and attain the energy efficiency that motivated the use of a compression algorithm in the first place. Therefore, a number of data compression methods specifically designed for WSNs have been proposed in the past few years [2]. What many of these methods have in common is the fact that they make use of the correlation of the data acquired by the sensor nodes in order to achieve high compression ratios while employing computationally inexpensive algorithms.

The remainder of this paper is organized as follows. Section 2 introduces the related work. In Section 3, the proposed protocol is specifically depicted, including its design idea and practical implement approach. The performance of the scheme is mainly evaluated in Section 5. Finally, in Section 6, we make some concluding remarks.

Related Work

Anurag [3] proposed the Energy efficient Secure Multipath Routing Protocol (EESM). It was divided into three phases Route construction, Transfer data and Route maintenance and security. It used the Ant Colony optimization algorithm for finding the shortest path between the sensor nodes. This source initiated (Base Station) protocol which uses public cryptography for secure the data and introduce the protocol schema to transfer the data from sink to source. Multipath routing protocol

was used for energy efficiency and security. The average energy consumption was calculated for data processing including authentication and average energy consumption for each bit of data transmitted.

Malika et.al [4] presented a new version of Directed Diffusion routing protocol which provides both security and energy efficiency together in wireless sensor networks. The choice of this protocol was motivated by the fact that it allows unicast and broadcast authentication and it is flexible in terms of energy consumption. LEAP protocol used four different keys to provide security in the network. But in this work, to secure Directed Diffusion and regarding to the different types of transmissions in this protocol, it was used the three different keys.

Kamal kumar et.al [5] proposed a new kind of multi path secure routing which distinguishes relays for query and reply, classified as Data-Relays (DRs) and Query-Relays (QRs). With provision of multiple DRs and QRs, the number of trials for successful traversal of packets from source to sink was reduced. The optimal selection of DRs in the network has been proposed, with objective of maximizing the Effective Average Keys on the routes from random node to sink. As the route was specified by sink and Forwarders are selected by nodes on the path, any masquerading and modification attack rendered ineffective. The analytical modeling supported the objectives and supports the strength of proposal.

Riad et.al [6] identified the WSN security trends and threats. It also addressed some examples of how to use artificial intelligence in the routing algorithms and shows the advantages and the drawbacks of each. A proposed framework also has been introduced.

Geeta and Chandrasekaran [7] proposed a trust management system where cryptography techniques fail to address some issues. The frame work for secure communication and trust management systems were proposed in this system. The simulation results are shown that the proposed model works for secure communication, data aggregation and intrusion. However, the proposed trust management system was suggested for various other applications.

Bijoy Kumar et.al [8] presented a secure routing protocol family for wireless sensor networks that builds atop the inherently attack-containing, dynamic binding. Rather than maintain routing tables, it chooses the next hop dynamically and none deterministically. This contains the effect of compromise to a local neighborhood, increases robustness to node mobility and failure, and spreads energy drain more evenly across neighbors. The open problem is left to design a sensor network routing protocol that satisfies our proposed security goals.

Di Tang et.al [9] proposed a novel secure and efficient Cost-Aware SEcure Routing (CASER) protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic-based random walking. The energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, an efficient non-uniform energy deployment strategy was proposed to optimize the lifetime and message delivery ratio under the

same energy resource and security requirement. It was also provided that a quantitative security analysis on the proposed routing protocol.

Deepa and Latha [10] proposed a high level scalability, security, cluster formation and cluster head selection for a hybrid secure routing protocol. The network life time can be increased gradually and the results were compared with the LEACH protocol. In the HHCS model, the sensor nodes were divided into smaller number of groups called as cluster. In each cluster, one sensor node acts as CH and other sensor nodes are act as a CM in level one. HHCS can reduce the energy consumption, improve the consistency of network energy and increase the life time of node in the network.

Pushpa Ragunath et.al [11] developed the system with security based on the Digital Signature and the security under digital signature. Initially nodes are grouped in the form of cluster and those clusters have the cluster head to access the region. After the formation of the cluster region, mobility was analyzed to process the data transmission. For the transmission of data, we propose the algorithm EEDC in the existing system. In the security part, there are two ways used i.e. identity based digital signature and Identity based online/offline Digital Signature. The system was proved with high security with present strategy.

Varsha and Jayashree Patil [12] proposed a security extension with the help of two techniques: Passive SET-IBS (Secure and efficient transmission in identity based signature) and active SET-IBOOS (Secure and efficient transmission in identity based online offline signature) technique using Diffie Hellman elliptical curve cryptography. In this work, a sensor network model was developed in Matlab to incorporate Physical-Mac layer fundamentals of modulation, channel error, transmission delay and bit error rate into the simulation to realistically analyze the behavior of this network and concept.

Surinderjit Kaur et.al [13] discussed and evaluated the performance of different techniques in different scenarios for mobile nodes by using Ad hoc On Demand Distance Vector (AODV) routing protocol for monitoring of critical conditions with the help of important metrics like delay, throughput and network load. In each scenario all the nodes were used as source nodes of sending data to a common base station. So according to the simulation the performance analysis of clustering technique is better in aspect of delay and throughput for mobile nodes. In aspect of network delay the performance of clustering technique with some failure nodes is better as compared to other scenarios. On selected techniques and protocol conducted study concludes that in overall performance clustering technique is better from other techniques.

Jose Anand and K. Sivachandar [14] discussed the routing protocol affected by vampire attack in WSN. This is a new class of resource consumption attack that use routing protocols to permanently disable ad-hoc WSNs by depleting node‟ s battery power. Simulation results have shown that depending on the location of adversary, network energy expenditure during the forwarding phase increasing. The security flaws of AODV can be fixed by using RSA encryption system that will avoid the adversary from entering the system.

Vaishali et.al [15] proposed two secure and efficient data transmission (SET) protocols for clustered Wireless sensor Network CWSNs, called SET-IBS by using

the identity-based digital signature (IBS) scheme and SET-IBOOS by using identity-based online/offline digital signature (IBOOS) scheme. This application facilitate to facilitate require packet Delivery from one or more senders to multiple receivers, provisioning security in group communications is pointed out as a critical and challenging goal In this research, a secure data transmission for cluster-based Wireless Sensor Network (CWSNs) was studied clearly.

Reshma Patil et.al [16] proposed the Secure Energy Efficient Routing (SEER) schema that consider cost of providing security and effects on energy efficiency. Secrete sharing method used for providing security. In this method information is divided into multiple shares and sends via multiple disjoint paths from source to destination at different point of time. At the destination end the original information reconstructed by combining the shares received via different paths at different point of time. It was also calculated the cost for security in term of time and its effect on energy efficiency.

Vikash Kumar et.al [17] introduced the concept of Wireless Sensor Network (WSN). The introductory section gives brief information on the WSN components and its architecture. Then it deals with some of the major security issues over wireless sensor networks (WSNs). This work also proposed some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications.

Shancang Li et.al [18] proposed Service-oriented architectures for wireless sensor networks (WSNs) to provide an integrated platform, where new applications can be rapidly developed through flexible service composition. In WSNs, the existing multipath routing schemes had demonstrated the effectiveness of traffic distribution over multipaths to fulfil the quality of service requirements of applications. However, the failure of links might significantly affect the transmission performance, scalability, reliability, and security of WSNs.

Roy.et.al [19] introduced a loss-resilient aggregation framework called synopsis diffusion, which uses duplicate-insensitive algorithms on top of multipath routing schemes to accurately compute aggregates (e.g., predicate count or sum). However, this aggregation framework does not address the problem of false sub aggregate values contributed by compromised nodes. This attack may cause large errors in the aggregate computed at the base station, which is the root node in the aggregation hierarchy. In this research work, it was made that the synopsis diffusion approach secure against the above attack launched by compromised nodes. In particular, it was presented an algorithm to enable the base station to securely compute predicate count or sum even in the presence of such an attack. The attack-resilient computation algorithm computed the true aggregate by filtering out the contributions of compromised nodes in the aggregation hierarchy.

Sohini Roy et.al [20] adopted a level based secure hierarchical approach to maintain the energy efficiency. It incorporates light-weight security mechanisms like, nested hash based message authentication codes (HMAC), Elliptic-Curve Diffie-Hellman (ECDH) key exchange scheme and Blowfish symmetric cipher. Simulation results were shown that the scheme performed better than existing secure routing protocols FBSR and ATSR.

In previous there was no stabilization between key generation and trust management introduced. It leads to high overhead, more resource consumption in Wireless Sensor Networks. There was lack of finding the malicious nodes from legitimate nodes.

Implementation of Proposed Trust Based Routing Mechanism

In WSNs In the proposed scheme, multipath route is deployed to improve the load balancing and network lifetime. The encryption and decryption scheme is proposed to provide both authentication and data integrity against the malicious activities. So each node can assure authenticated route as well as node. The following describes the proposed multipath and secure authentication scheme.

A. Proposed Multipath Routing Approach

In the proposed protocol, nodes are randomly distributed in a large area, since some dense nodes are located in the smaller area. Multipath is generated from source to destination node by means of configuring the link quality and capacity. Only one node can be the member of multiple paths even though other members are supposed to be the potential member of paths. Updating cache/reward case in routing tale of cluster head or source node is not conductive in some special cases. For an example, the nodes in region 1 can communicate with nodes in region 2. When node 3 and node 4 receive the forward investigations from node 2 and node 1, the cache is updated quickly and consider node 1 as the previous node because the popularity from node 1 is of maximum value. For the same case, other nodes in region 2 all choose node 1 as the previous hop. The popularity of node 2 is very close to that of node 1, although the former is less than the latter. It is identified that the node 2 is not able to become the intermediate node of any path inside the region. Here, some potential paths are dropped. By considering the above criteria the improvement to cache update is as follows. It is assumed that R_1 is the popularity along path 1, which is recorded in node 3. R_2 is the newly received popularity along path 2.When $R_2 \gg R_1$, node 3 updates the popularity value and the previous hop entry in the cache. And when $R_2 \ll R_1$, node 3 does not update the cache. Only when R_1 and R_2 meet the following formula:

$$\frac{|R_1 - R_2|}{R_1} \leq \chi \tag{1}$$

Where χ is the relative difference, and it is approximately equal to 0.05, the cache will be updated with the probability p given by,

$$p = \begin{cases} \left(\dfrac{R_2}{R_1 + R_2}\right)^2 & (R_2 \leq R_1) \\ \sqrt{R_2 / R_1 + R_2} & (R_2 > R_1) \end{cases} \tag{2}$$

Based on the above condition, some potential paths may be built. Any path with higher stability can be established via initial node. It contributes to the energy consumption balancing and the prolonging of the network lifetime. At last, node may

be in the position of neighbor to sink may choose other neighbor to sink as the previous hop. It leads to decrease the number of paths and results in quick fade of neighbor nodes near the sink. If Node D receives the forward investigate from node B and node C, it choose node B as the previous hop due to the node B's higher popularity. If more hops are found while the path covering node C, it leads to lower popularity. When the backward investigates travel back, the potential path which passes sink, node D, node B and node A in sequence will be discarded. During some critical situations, the other neighbor nodes of sink may encounter the same situation, especially when the source node is far away from sink. In order to solve the problem above, the method is proposed that the node will directly send the forward investigates to sink instead of broadcasting only when the node is the neighbor of sink. All the nodes near sink is connected through the stable link.

B. Proposed Data Compression Method

The following steps illustrate the network model of proposed compression method.

Step 1: Consider a sensor node which is used to monitor the environmental data.

Step 2: Sensor node acquires the data at any time instant once analog to digital conversion is made.

Step 3: Represent the each symbol $x_k \in \chi$ with an k bits long codeword. Average number of bits used to represent each symbol is given by $L = \sum_{i=0}^{N-1} p_i k_i$.

Step 4: Set the theoretical limit for the minimum number of bits/symbol for a discrete source is the source entropy.

$$H(\chi) = \sum_{m=0}^{N-1} p_m I_m = \sum_{m=0}^{N-1} p_m \log_z (p_m) \tag{3}$$

Where I_m is the information measure of source symbol x_m.

The output efficiency of a proposed compression can be measured by comparing the average symbol length after compression to the source entropy. The main objective is to devise a simple compression method which approaches the performance of optimal entropy coding while relying on a fixed database. After comparing the probability distribution of the link capacity and of the differences of consecutive capacities for many datasets of measurements carried out at different locations, we noticed that the distributions of the differences are quite similar for all datasets, even though the distributions of the temperature values vary significantly. A fixed alphabet construction is obtained by the application of the Huffman algorithm to a large dataset of temperature measurements. We consider Set 1 as our reference dataset, without any particular reason other than the fact that both the number of samples and the measured temperature range are quite large. This approach uses a reference dataset to generate a database for a particular parameter under observation. The frequencies of each of the symbols available in the reference dataset are compared to construct the Huffman tree that represents the compression alphabet.

In the proposed compression scheme, there are two special cases considered i.e.

(i) During data collection period, the first sample, x_0, must be transmitted uncompressed since there is no previous measurement to compute the

difference d_0. From the second sample on, the differences d can be properly computed and compressed.

(ii) Limited range of difference values covers according to the data available in the reference dataset. However, the probability of occurrence of a symbol not present in the database is extremely low. Hence, its value can be sent uncompressed and identified by the presence of a special marker in the Huffman dictionary. If a codeword is not part of the original database and whose presence can be unmistakably detected may be transmitted to signify that the next symbol corresponds to an uncompressed value, which can then be transmitted using a subsequent codeword of a fixed previously defined length.

C. Secure Routing Approach

In the proposed secure routing the compressed data is encrypted with private key and decrypted with public key, to secure network information. A redundancy function R from the message space M to M_s is selected and is public knowledge.

Summary:

each entity creates a public key and corresponding private key.

Each entity A should do the following:

1. Generate two large distinct random primes p and q, each roughly the same size.
2. Compute n = pq.
3. A's public key is n; A's private key is (p, q).

Summary

entity A signs a message m ∈ M. Any entity B can verify A's signature and recover the message m from the signature.

1. *Signature generation.* Entity A should do the following:

a) Compute $\overline{m}$ = R(m).
b) Compute a square root s of _m mod n.
c) A's signature for m is s.

Verification. To verify A's signature s and recover the message m, B should:

a) Obtain A's authentic public key n.
b) Compute $\overline{m} = s^2$ mod n.
c) Verify that $\overline{m} \in$M; if not, reject the signature.
d) Recover m = R ($\overline{m}$).

D. Energy Consumption Model

Let the energy consumption per packet is taken as E_{Pac}. It includes both transmission and reception energy. The total energy consumption of a network is calculated as,

$$E = E_{tx} + E_{rx} + E_{path} = n_{tx} \times e_{tx} + n_{rx} \times e_{rx} + n_{tr} \times e_{path} \quad (4)$$

In the above equation (3.1), the n_{tx} and n_{rx} are the number of transmission and receptions respectively, where as n_{tr} is the number of both transmissions and receptions occurred in a path at a time. e_{tx},e_{rx},e_{path} are the energy spent on transmission, reception and path.

$$e_{tx} = E_{em} \text{ x } K + \chi_{amp} \text{ x } K \text{ x } d^2 \quad (5)$$

K = bit which consists of current energy level of the node, path, data label, node's location and hop count.

E_{elec} = transmitted and Received energy on electronic device module (40 nJ/bit).

χ_{amp} = Transmitter Amplifier (100 pJ/bit/m^2)

d = distance between the two mobile nodes.

And the energy for receiving K bit is equal to:

$$e_{rx} = E_{em} \text{ x } K \quad (6)$$

If choosing the path with minimum energy consumption, the energy efficiency of the network will be more improved.

In energy consumption model, there are four metrics are considered based on energy i.e. stability of multipath, link stability, energy spent on communication phase and link availability. In routing table, all the nodes energy status are calculated before and after transmission.

D. Proposed packet format

Source ID	Destination ID	Authentication Status	Packet Integrity Status	Energy Conservation Rate	CRC
2	2	4	4	4	2

Figure 1: Proposed Packet format

In figure 1. the proposed packet format is shown. Here the source and destination node ID carries 2 bytes. Third one is authentication status of the node. The authentication status induces the whether the transmission of packets are travelled through authenticated route. In fourth field, the packet integrity status is indicated. It determines how much of the genuine packets are transmitted between source and destination node. It also determines whether packet contains authorized information. In fifth, the energy conservation ratio is allotted to ensure minimum energy consumption. The last filed CRC i.e. Cyclic Redundancy Check which is for error correction and detection in packet while route maintenance process.

Performance Evaluation

A. Simulation Model and Parameters

Based on simulation performance, the proposed system can withstand the chosen cipher text attacks, Sybil attack, sink hole attack and other passive attacks etc. In previous work, there was no reliability on trust management system. The analytical model was not proved for attackers in the previous work. The proposed key based authentication protocol is simulated with Network Simulator tool (NS 2.34). In our simulation, 100 sensor nodes move in a 1300 meter x 1300 meter square region for 100 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 200 meters. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1.

Table 1: Simulation Settings and Parameters

No. of Nodes	100
Area Size	1300 X 1300
Mac	802.11
Radio Range	200m
Simulation Time	100 sec
Traffic Source	CBR & Poisson
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	LEACH

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Control Overhead: Ratio of control packets to the data packets received.

The simulation results are presented in the next part. We compare our proposed protocol ECSAP with LZW-HIGHT [22], ADLC [21] and SFA [19] in presence of random mobility environment.

C. Results

Nodes actual behaviors comply with the Bernoulli trial, which means that the probability that a node acts good is predetermined. If a node acts well for less than 30 percent of the interactions, it is considered as a malicious node. The default percentage of malicious node in the network is 10 percent.

In our First experiment, we vary pause time as 20, 30 up to 100. Figure 2 show the results of delivery ratio for the nodes compressed bytes. Clearly our scheme achieves more delivery rate than the previous schemes. The proposed scheme contains load

balancing method to identify legitimate nodes and forward the packets through the nodes. So packet delivered at the destination is more.

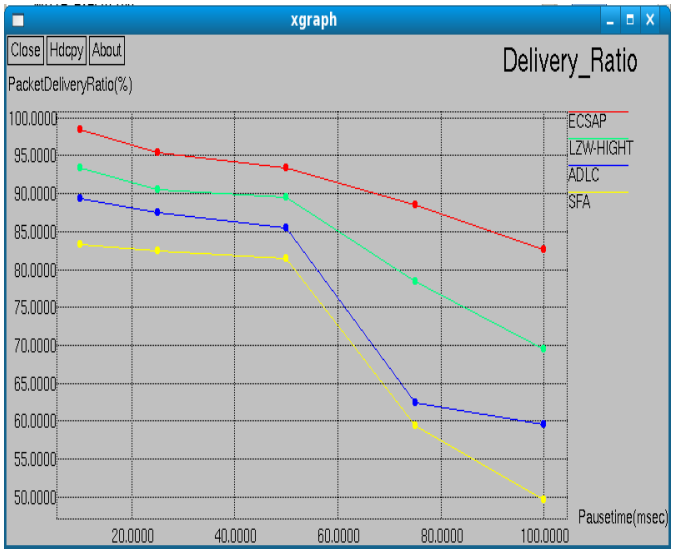

Figure 2: Delivery Ratio Vs Pause time

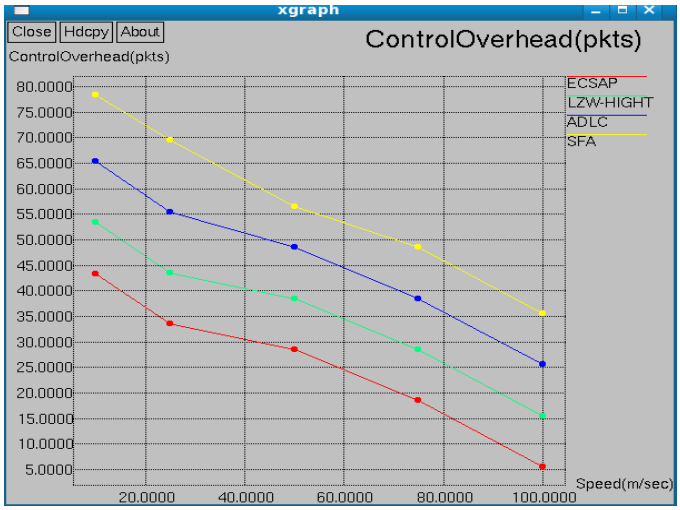

Figure 3: Control Overhead Vs Speed

Figure 3 shows the results of Control overhead Vs Speed. From the results, we can see that proposed secure routing protocol achieves less overhead than previous schemes. It is because of link capacity improvement. The complexity of compressed bytes is very less to achieve minimum overhead.

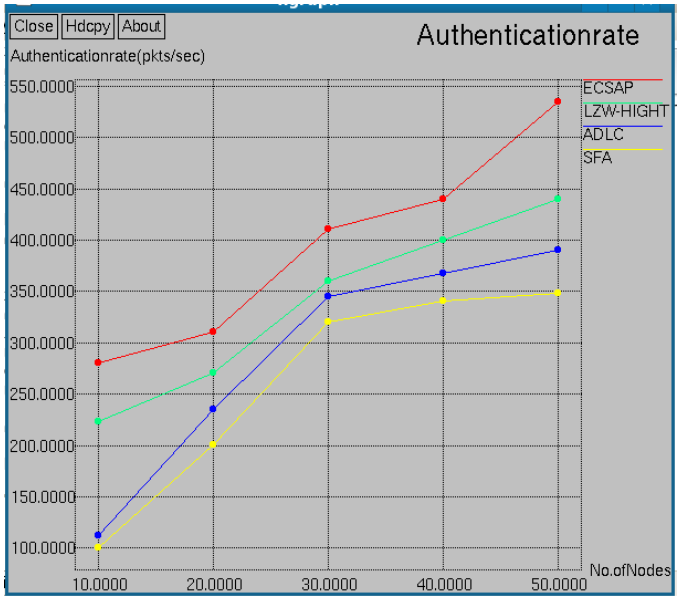

Figure 4: Authentication Rate Vs No. of Nodes

Figure 4 shows the results of Authentication rate for the 100 node scenarios. Clearly our system achieves high authentication rate than previous data compression methods. The proposed system comprises two major aspects i.e. Data compression and data authentication process. Packet is delivered via reliable nodes through stable link.

Figure 5 shows the results of Memory Requirement Vs No. of Nodes. From the results, we can see that proposed protocol achieves less memory requirement than previous systems because of Huffman data compression method.

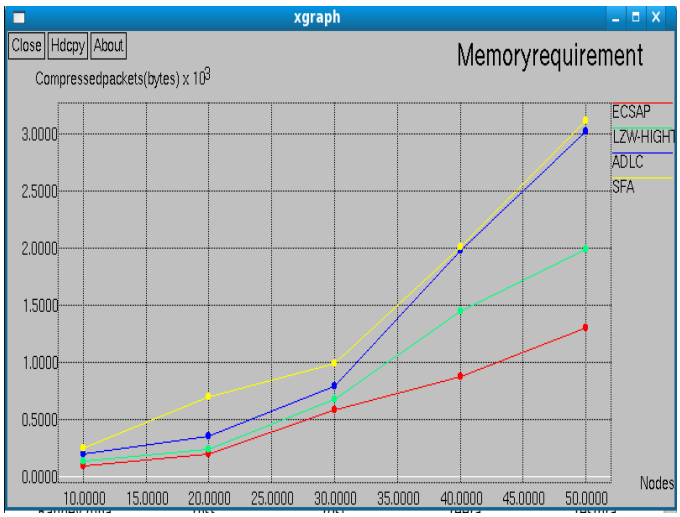

Figure 5: Memory Requirement Vs No. of Nodes

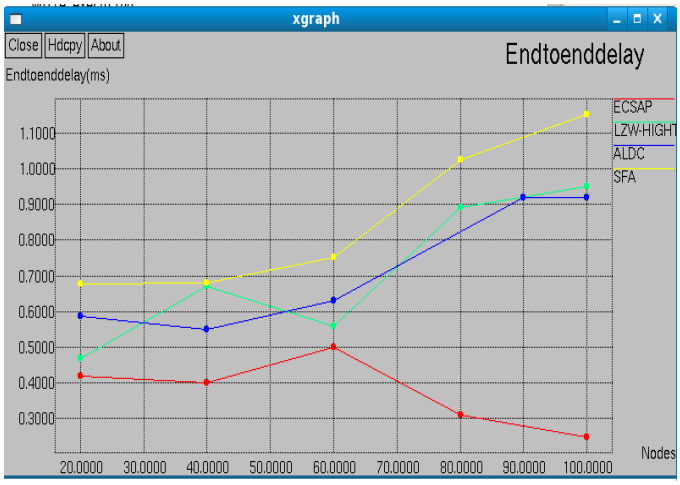

Figure 6: End to end delay Vs No. of Nodes

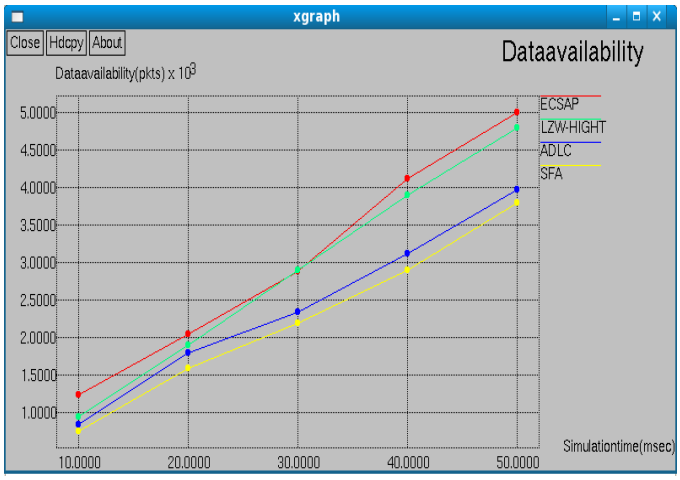

Figure 7: Data availability Vs Simulation time

Figure 6 shows the results of End to end delay Vs No. of Nodes. From the results, we can see that proposed protocol achieves less delay than previous systems because of channel quality and reliable link selection.

Figure 7 shows the results of Data availability Vs simulation time. From the results, we can see that proposed system has more data packets available to destination based on demand while comparing to the other previous systems. The proposed system increases packet availability using load balancing approach.

Conclusion

This paper presents the secure data compression method based on fixed Huffman database. In this proposed scheme ECSAP is designed for making balance between compressed data and authentication status. Nodes are chosen based on popularity and

connectivity is established based on link stability. Multipath is demonstrated to achieve potential network stability. Packets are encrypted and decrypted with symmetric encryption model. Energy consumption model is introduced to maintain power consumption with minimum level. Based on the simulation results, the proposed scheme achieves better performance than existing schemes in terms of performance metrics.

In future work, we have planned to include energy consumption model with checkpoint routing to achieve optimized network performance.

References

[1] T. Srisooksai, K. Keamarungsi, P. Lamsrichan, and K. Araki, "Practical data compression in wireless sensor networks: a survey," Journal of Network and Computer Applications, vol. 35, no. 1, pp. 37–59, 2012.

[2] F.Marcelloni and M.Vecchio, "Asimple algorithmfor data compression in wireless sensor networks," IEEE Communications Letters, vol. 12, no. 6, pp. 411–413, 2008.

[3] Anurag, "Energy Efficient Secure Routing Algorithm for Wireless Sensor Networks", Proceedings of Twelveth IRF International Conference, 2014,pp.90-93.

[4] Malika Belkadi, Rachida Aoudjit, Mehammed Daoui, Mustapha Lalam, "Energy-efficient Secure Directed Diffusion Protocol for Wireless Sensor Networks", International Journal of Information Technology and Computer Science, 2014, 01, pp.50-56.

[5] Kamal Kumar, A. K. Verma and R. B. Patel, "Secure Multipath Routing Scheme Using Key Pre-distribution in wireless sensor Networks", International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.4, No.4, July 2014, pp.49-61.

[6] M. Riad, Hamdy K. El-Minir and Mohamed El-hoseny, " Secure Routing in Wireless Sensor Networks: A State of the Art", International Journal of Computer Applications, Volume 67– No.7, April 2013, pp.7-12.

[7] Geetha V., K. Chandrasekaran, "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network", Wireless Sensor Network, Vol.6, 2014, pp.173-183.

[8] Bijoy Kumar Mandal, Debnath Bhattacharyya and Kil-hwan Shin, "A Security Architecture for Wireless Sensor Networks Environmental", Contemporary Engineering Sciences, Vol. 7, 2014, No. 15, pp.737 – 742.

[9] Di Tang, Tongtong Li, Jian Ren and Jie Wu, "Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks", IEEE Transactions on Parallel Systems, pp.1-13.

[10] Deepa and B. Latha, "HHCS: Hybrid Hierarchical Cluster Based Secure Routing Protocol for Wireless Sensor Networks", ICICES 2014, pp.1-6.

[11] R.Pushpa Raghunath, K.Venice Christopher, R.Vignesh, S.Deepika and M.Radhamani, "Effective and Secure Transmission Approach for Multi

Cluster Based Wireless Sensor Network", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue 3, 2014, pp.3277-3281.

[12] Varsha .S. Chare and Dr. Jayashree.Patil, " Secure and efficient data transmission in wireless sensor networks using elliptical curve cryptography", International Journal of Advanced Research in Computer Engineering & Technology, Volume 3 Issue 7, July 2014, pp.2416-2423.

[13] Surinderjit Kaur, Mrs. Amrit Kaur and Kiranveer Kaur, " Improved Secure Routing Scheme with Encrypted Session keys in WSN", International Journal of Emerging Research in Management &Technology, Vol.3, Issue 3, 2014, pp.6-16.

[14] Jose Anand and K. Sivachandar, " Vampire Attack Detection in Wireless Sensor Network", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, July 2014, pp.639-644.

[15] Miss. Vaishali M.Sawale1, Prof. Arvind.S.Kapse, "Enhanced Data Transmission for Cluster-Based Wireless Sensor Networks", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 3, March 2014, pg.453 – 457.

[16] Reshma Patil, Prof.S.M.Shinde, " Secure Energy Efficient Routing in Wireless Sensor Network", International Journal of Computer Technology & Applications,Vol 5 (4), pp.1392-1397.

[17] Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology. Volume 4, Number 8 (2014), pp. 859-868.

[18] Shancang Li ; Coll. of Eng., Swansea Univ., Swansea, UK ; Shanshan Zhao ; Xinheng Wang ; Kewang Zhang, "Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks", IEEE systems Journal, Vol.8, Issue 3, 2014, pp.858-867.

[19] Roy, S., Kansas State Univ. Conti, M. Setia, S. Jajodia, S., "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions on Forensics and Security, Vol.9, Issue 4, 2014, pp.681-694.

[20] Sohini Roy, Ayan Kumar Das, "Secure Hierarchical Routing Protocol (SHRP) for Wireless Sensor Network", Security in Computing and Communications in Computer and Information Science, Springer, Volume 467, 2014, pp 20-29.

[21] Jonathan Gana Kolo, S. Anandan Shanmugam,DavidWee Gin Lim, Li-Minn Ang, and Kah Phooi Seng, "An Adaptive Lossless Data Compression Scheme for Wireless Sensor Networks", Journal of Sensors, 2012, pp.1-21.

[22] Anshad.a.s, dr. R. Radhakrishnan, " Enhanced energy management inWSN using LZW security algorithm", pp.1-4.

Author Details

Mr.Anshad.A.S.,M.E.,is a research scholar in ECE Department of Sathyabama University, Chennai. He is an Assistant Professor in ECE Department of Malabar College of Engineering and Technology, Thrissur, Kerala. He graduated in Electronics from Kerala University, Thiruvanathapuram, and received M.E. from Sathyabama University, Chennai. His research interests are wireless sensor networks and wireless communication. He has been qualified the National Eligibility Test (NET) conducted by UGC in June 2014.

Dr. R.Radhakrishnan was graduated from Bharadhidasan University in Electronics and Communication Engineering and had done his Masters in Applied Electronics from PSG Tech, Bharathiar University and Ph.D from Anna University, Chennai. Having teaching experience of over 24 years with wide experience in research. He started his teaching career at Sri Ramakrishna Engineering College and served at various capacities. His areas of research are Wireless Networks, Microprocessors and Microcontrollers and Computer Networks. Three Ph.D candidates have completed their work under him. He has published over 50 technical papers in National and International Journals/Conferences.