IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

An Energy Monitored and Route Coded Based Wireless Sensor Network for Assurance of Quality of Service

Amruta Padhye[1], Shraddha Panbude[2]

Student, EXTC, VIT, Wadala, Mumbai, India [1]

Assistant Professer, EXTC, VIT, Wadala, Mumbai, India [2]

Abstract: WSN (Wireless Sensor Network) is widely employed in various fields because of its terrific performance, such as in the public health service, agricultural technology and environment monitoring. Due to the complex requirement of environment monitoring and the restricted energy of each node, reducing power consumption and reliable transmission are vital issues in the research areas of wireless senor network. The field of wireless networking technology is emerges from the integration of personal and private computing, cellular technology, and the Internet. This is due increase interactions between communication and information data computing, which is changing information access from "anywhere, anytime" into" everyplace, all the time". With the accumulated demand and application of wireless sensor networks (WSNs) to military and civilian fields, data security in the network has become a critical issue. The serious resource constraints of sensor nodes and all so the broadcasting nature of the wireless links as well as difficulties in the deployment environments of wireless sensor networks cause challenges for the quality and security of data transmission for these wireless networks. In order to ensure data security and quality of service required by an application in energy efficient and power saving way, we are proposing a new mechanism for QoS routing with coding and selective encryption scheme for WSNs. Our approach provides secure and reliable data transmission and can also adapt to the varied resource constraints of WSNs. The original message is splits into packets and they are coded and selectively encrypted before being transmitted along completely different disjoint paths.

Keywords: Wireless Sensor Network (WSN), Quality of Service (QoS), Energy Efficient WSN, coding.

I. INTRODUCTION

Recent technological improvements have made the deployment of small, inexpensive, low-power, distributed devices, which are capable of local processing and wireless communication, a reality. Such nodes are called as sensor nodes. Each sensor node is capable of only a limited amount of processing. But when coordinated with the information from a large number of other nodes, they have the ability to measure a given physical environment in great detail. Thus, a sensor network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. Sensor networks are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. Wireless sensor networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a variety of fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment. As a complex network consisting of sensing, processing and communication wireless network is driven by various applications and highly required a new quality of service guarantees. A common approach to satisfy some QoS requirements in Wireless Sensor Networks (WSNs) is to use forward error correction (FEC) technique as a replication mechanism in multipath routing to increase data transmission reliability, decrease energy consumption and increase network lifetime while avoiding the costly or impossible data retransmission due to the severe resource constraints of sensor nodes . Routing is an essential problem in any type of networks. Compared with existing routing protocols, secure routing for WSNs is a very challenging task due to the severe resource constraints of sensor nodes; the broadcast nature of the wireless links makes the WSNs vulnerable to link attacks that include passive eavesdropping, active impersonation, and message replay and message distortion, dynamically changing in the size and density of the network, as well as the high risk of physical attacks to sensors. Due to this people are thinking about, a new mechanism is proposed that adapts to the resource constraints of WSNs by combing FEC technique and selective cryptographic algorithms (AES) to achieve both reliable and secure data transmission in WSNs. The original message is split into packets that are first coded using RS codes. Then depending on the required security level, the selective encryption scheme is used to encrypt selected number of fragments on each codeword before being transmitted along different disjoint paths.

Thus the security can be achieved while respecting the resource constraints of WSNs. Reed-Solomon codes are examples of error correcting codes, in which redundant information is added to data so that it can be recovered

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

reliably despite errors in transmission or storage and retrieval.

II. LITERATURE REVIEW

The traditional encryption algorithms which were used earlier were too complex and introduce many delays in nodes [1]. Cryptography schemes are typically used to meet the basic security requirements in networks. But as the sensor nodes are limited in their computational and memory capabilities, the well-known traditional cryptographic techniques cannot be merely transferred to WSNs without adapting them [6]. Symmetric and Asymmetric encryption and decryption are basic traditional algorithm are available for security in the network. In asymmetric encryption is uses two related keys (public and private) for data encoding and decoding, and takes away the safety risk of key sharing. The private key is never exposed. The message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. Likewise, a message that's encrypted by the private key can only be decrypted by using the matching public key. Examples are RSA, ECC etc [6].

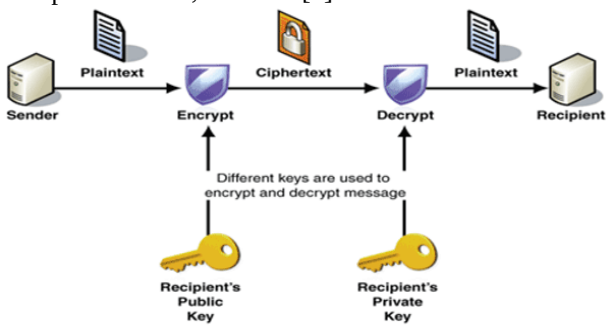

Fig 1: Asymmetric Key Cryptography

The cryptographic algorithm RSA is presently the most used among the asymmetric algorithms, working from the difficulty of factoring large prime numbers. A user of RSA creates so publishes a public key based on two large prime number, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message. Breaking RSA encryption is known as the RSA problem. RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. Symmetric algorithms uses the same secret key for encryption and decryption where asymmetric uses different keys for the same. Asymmetric key encryption, on the other hand, makes use of two keys. A private key and a public key. The public key is used for encrypting, while the private key is used for decrypting. Asymmetric key consumes more energy and it is more expensive as compared to symmetric key. public key consumes more energy due to great deal of computation and processing involved ,which makes it more energy consumptive as compared to symmetric key technique e.g. a single public key operation can consume same amount of time and energy as encrypting tens of megabits using a secret key cipher[6]. The more consumption of computational resources of public key techniques is due to the fact that it uses two keys. One of which is public and is used for encryption ,and everyone can encrypt a message with it and other is private on which only decryption takes place and both the keys has a mathematical link, the private key can be derived from a public key. In order to protect it from attacker the derivation of private key from public is made difficult as possible like taking factor of a large number which makes it impossible computationally. Hence, it shows that more computation is involved in asymmetric key techniques thus we can say that symmetric key is better to choose for WSN. The cost of public key is much more expensive a s compared to symmetric key for instance, a 64 bit RC5 encryption on AT mega 128 8 MHZ takes 5.6 milliseconds, and a 160 bit SHA1 function evaluation takes only 7.2 millisecond's. .These symmetric key algorithms are more than 200 times faster than Public key algorithms. Symmetric encryption (also called as secret-key cryptography) uses a single secret key for both encryption and decryption.

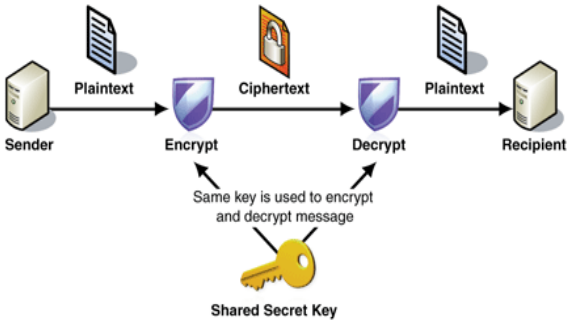

Fig 2: Symmetric Key Cryptography

This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used to achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated [6]. Examples are AES; 3DES etc. symmetric cryptography has a higher effectiveness and requires less energy consumption. Due to this we use FEC with selective cryptographic algorithm for secure data transmission as the forward error correcting codes are less complicated and easy to use code for coding [1].

A lot of research has been done on some important aspects of WSNs such as architecture and protocol design, energy conservation, and locationing, supporting Quality of Service (QoS) in WSNs is still a largely unexplored research field [7]. This is mainly because WSNs are very different from traditional networks. QoS generally refers to the quality as perceived by the user/application while in the networking community; QoS is accepted as a measure of the service quality that the network offers to the applications/users [7]. The QoS mechanism should improve the efficiency and reduced the energy consumption of sensor nodes to delay the network survival time. Requirements of QoS in WSN are different from

DOI 10.17148/IJARCCE.2016.5138

wired networks. Traditional end-to-end QoS parameters may not be sufficient. As a result, new parameters are used to measure the QoS performance in WSN [8].While especially in wireless sensor network, many QoS based routing protocols have been proposed but they normally make their primary metrics to energy consumption.

The basic problem, therefore, is to find a path that satisfies the multiple constraints for QoS routing in an energy-efficient way. Though the single-path routing is simple and less energy consuming as compared to the multipath routing, the failure of the transmission path may break the link and completely ruin the delivery. In multipath transmission the data packet is transmit through multiple links so is avoid costly retransmission of packet which can save energy of the node at the same time provide guaranteed delivery [8]. To overcome these difficulties we proposed a mechanism to save energy which also satisfies the requirement of QoS.

III. PROPOSED SYSTEM

The severe resource constraints of sensor nodes and the broadcast nature of the wireless links as well as the challenging deployment environments of wireless sensor networks pose challenges for the quality and security of data transmission for these networks.By combing FEC technique and selective cryptographic algorithms to achieve both reliable and secure data transmission in WSNs. In the proposed protocol, RS coding is used to provide reliability and security. The sink node decides on the paths selection process in order to satisfy the reliability or the delay requirements by an application and the number of these paths is determined to enhance the reliability.

A. Project Algorithm Steps

The project objectives and algorithms are mentioned below.

1) Creating a network with 200 nodes for simulation we can select any number of nodes out of 200.
2) Generate random motion topology using random way point.
3) Select source and destination ids.
4) Employ coding technique for routing to increase the QoS .
5) Compare energy value of node with threshold value (say 2dBm), if node energy is greater than this then we can proceed for the routing.
6) Evaluate the system using performance parameters such as packet delivery ratio, end to end delay, energy consumption and average life time of node.

B. Performance Parameter.

1. Average lifetime of a node: This gives a good measure of the network lifetime.
2. Average delay per packet: the average time a packet takes from a sensor node to the gateway.
3. Network throughput: Defined as the total number of data packets received at the gateway divided by the simulation time.
4. Packet delivery ratio: It is known as pdr.It gives ratio of packets delivered from source to destination in a system.

IV. CONCLUSION

This paper is basically focuses on the traditional encryption algorithms present for security and quality of service for proper routing of data packets within the wireless sensor network.In this project; we presented a new routing mechanism, which integrates FEC codes and selective encryption scheme for providing both QoS and secure data transmission in WSN. We will be developing the proposed technique.

REFERENCES

[1] Hind Alwan, and Anjali Agarwal,"a secure mechanism for qos routing in wireless sensor networks",2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).
[2] A.Wood, and J. Stankovic, "AMSecure: Secure link-layer communication in TinyOS for IEEE 802.15.4-based wireless sensor Networks," In proceedings of the fourth International Conference of Embedded Networked Sensor systems, New York, USA, pp. 395–396, 2006.
[3] E. Stavroua, and A. Pitsillidesa, "A Survey on Secure Multipath Routing Protocols in WSNs," Computer Networks, Vol. 54(13), pp. 2215-2238, 2010.
[4] S. K. Singh, M.P. Singh, and D.K. Singh, "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks," International Journal of Computer Trends and Technology, Vol. 1(2), pp. 9-17, 2011.
[5] R. Ma, L. Xing, and H.E. Michel, "A New Mechanism for Achieving Secure and Reliable Data Transmission in Wireless Sensor Networks," In proceedings of the 2007 IEEE Conference on Technologies for Homeland Security.
[6] Madhumita Panda,"Security in Wireless sensor network using cryptographic technique", American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, Issue-01, pp-50-56.
[7] Dazhi Chen and Pramod K. Varshney ," QoS Support in Wireless Sensor Networks: A Survey "Department of EECS, Syracuse University Syracuse, NY, U.S.A 13244
[8] Noor Zaman,Abdul Raouf Khan,Mohammad Salih" Designing of Energy aware Quality of Service (QoS) based routing protocol for Efficiency Improvement in Wireless Sensor Network (WSN)" Journal of Information & Communication Technology Vol. 4, No. 1, (Spring 2010) 19-37.
[9] Di Tian, Nicolas D. Georganas," Energy Efficient Routing with Guaranteed Delivery in Wireless Sensor Networks"IEEE wireless and networking conference 2003.ISSN 1525-3511.