International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 29147-29154

http://www.ripublication.com

Secure Emergency Response Protocol For Wireless Sensor Networks

A. Deepika
M. Tech 2nd year, department of CSE
SVEC, Tirupati, AP, India
deepika.ampati@gmail.com

Abstract

Wireless sensor networks are those in which nodes are distributed randomly in order to pass the information from one sensor node to another node. Emergency responses are uncommon in a communication network. Adaptation to topological changes, coping with heavy traffic, and automatically switching from normal mode to energy efficient mode are the emergency responses that are to be met. The emergency response protocol tackles all these problems but security is the major concern which is an important aspect for preventing an attacker from automatically changing the network into emergency mode so that nodes energy is reduced and also packets in the queue are duplicated with improper data. Simulations in NS-2 show the improvement in the performance in packet delivery ratio, delay and energy in normal monitoring.

Keywords: Emergency responses, security, normal mode, emergency mode, slack time.

Introduction

A WSN mainly comprises of randomly distributed sensor nodes which are employed to predict the changes in the environment and organized for passing the collected information to the destination. The nodes in WSN posses certain capabilities such as sensing, computation and communication.WSN is a small part of ad-hoc networks which provide mobility parameters for the nodes in the network. Although WSN is a division of ad-hoc networks the protocols used in WSN are not used in ad-hoc networks.

Communications can be done in different layers but mainly a protocol is designed in a medium access control layer that is meant for controlling the interfering properties of the nodes in transmissions. In WSN energy management of nodes in MAC layer is very difficult, so while designing a protocol one should be careful that

the energy of a node should not deplete. In an emergency situation, the nodes should respond immediately to stop the disasters such as fire condition, earthquakes etc.

The existing protocols are not capable of handling the large amounts of traffic, healthy adaptation to changes, packet prioritization and completeness. Currently, the medium access control that is designed for WSN is divided into contention based protocols and TDMA related protocols. TDMA protocols have an advantage of energy minimization compared to contention protocols, because the number of cycles is reduced and there is no contention. By using this nodes can share the same frequency channel through the division of signal into different time slots. When the transmission starts, the nodes use their time slot, and allow multiple stations to use same transmission medium.

The advantages of WSN are complexity of wiring is avoided; changes can be easily adapted, very flexible to divide physical partitions. The major drawbacks are low speed of communication, more complex to configure than a wired network, costs are heavy. The major applications are intrusion detection, health application and traffic analysis to minimize the congestion.

Related Work

Eminent research has to be done to enable efficient communication in WSN because emergency responses are difficult to generate. Many MAC protocols are designed for WSN's, a classification of protocols that are related to the specific problem is selected which can adapt to topology changes and handling heavy traffic. Based on the mechanisms to access the medium for data transmission, classification of MAC protocols is considered. The major problems with existing protocols are collisions, protocol overhead and overhearing.

The contention based MAC protocols are generally used for detecting the collisions over the network. To obtain channel all the nodes compete with each other to greatly improve by sensing the medium before the packet arrival. It avoids this by using three policies like interface space, the contention window and acknowledgement. The major use of this kind of protocol is to increase scalability and adaptability. Some examples of contention based protocols are Sensor, Timeout, Berkeley, Wise-MACS.

Time division multiple access has an advantage of clashing among the nodes is avoided. Since the collision is avoided energy wastage due to collision is greatly reduced. Hybrid MAC is a combination contention-based and TDMA. The major limitations of these protocols are as follows:

1. Cannot cope with large amounts of traffic and larger test-beds .
2. Maximum trade-off between energy consumption and overall throughput.
3. Fast end-to-end delivery of packets is very low.
4. Implementation of these protocols is difficult on the devices have very limited computational resources.
5. Relocation and mobility of the gateway under QoS traffic are not addressed.
6. Cross layer architectures should be designed based on the application requirements.

Problem Definition

The most important problem in the existing MAC protocols is energy efficiency, through put, latency and network security. In this paper by designing emergency response protocol all the problems are tackled. The major functionalities of this protocol are as follows:

1. Consider a tree which gathers data with a source as the root of the tree and obtain neighborhood connectivity.
2. Assign and schedule the nodes by the TDMA slot assignments.
3. Managing time synchronization to minimize clock skews.
4. Consider two priority queues for en-queuing the packets.
5. Responding to emergency situations by changing properties of node in order to handle with large amounts of traffic.

Normally when packets are sent from source to destination one may fill the packets in the priority queue with improper data. By the duplication of data in packets the nodes can change their behavior normal to emergency monitoring which results in wastage of energy because nodes goes on processing in order to analyze where really the emergency occurs. To reduce these scenarios a network security mechanism called Elliptical Curve Cryptography has to be developed that can take random values so that the performance parameters should not deviate.

Proposed System

The emergency response protocol has two modes of monitoring; one is normal monitoring in which nodes will be in sleep mode and wake up when there is transmission and reception process. This mode is delay tolerant and cannot cope with heavy traffic. But in the emergency monitoring, when the node detects any emergency situation move towards the source node to notify the changes in the network. If any node is very far from the source then it may use two hop counts to notify the source node. The mobility of a node is set in their node properties and behavior is also prescribed. The intermediate nodes are not used in order to avoid delay, energy and also throughput. In the emergency mode only high priority packets are passed through the network. The differentiation can be done using the slack time, the packet which has lowest slack should be delivered first and if the slack time expires the packet will be lost.

As specified earlier, in order to prevent an attacker from changing the network from normal to emergency mode and to stop the duplication of packets elliptical curve cryptography algorithm is introduced which encrypts the packets with a sender's public key before queuing and when the packets reach its destination decryption is done by the receiver's private key. The algorithm generates two cipher texts for the purpose of tight security in the network. It can be added in the protocol after the channel access and before the placing the packets in the queue. The following steps depict the process of the proposed system:

- Establish the network consisting of thirty nodes.
- By using CSMA/CA, communication among the nodes is established.
- By using TDMA, slots are assigned and scheduled in the nodes.

- Two queues are used for the packets one for priority packets and one for low priority packets.
- Encrypt the packets and start sending them to their destination nodes.
- If an emergency is detected, nodes change their behavior from normal to emergency in order to cope with heavy traffic and topological changes.
- By the simulations average energy consumption, packet delivery ratio and average latency are calculated.

Algorithm:
Elliptical curve cryptography
Input: Message to send.
Output: Receive message.

Step1: Calculating the possible values for getting the elliptical curve by using following equation.

$Y=x^3+x+1$

Step2: Generation of public key

Q=d*p
Where d= private key ranging from 1 to n-1
p= point on the curve

Step3: Encryption

C1=k*p
C2=M + k*Q
Where C1,C2= Cipher texts
k= random integer ranging from 1 to n-1
M= Message
Q= Public key

Step4: M=C2-d*C1

This is the algorithm of elliptical curve cryptography as depicted above and now just checks the efficiency of this algorithm in the following way.

Let the message to be sent is HI
ASCII value of HI=9495
Consider a point on the curve by taking x –coordinate as 0 then $Y=x^3+x+1$, we get Y=1
So (0,1) is the point.
Public key generation:
Q=d*p
Here we take value of n=10 then d=9 and p=(0,1)
We get Q=9
Encryption:
C1=k*p
k=3,p=(0,1) we get C1=3

C2=M + k*Q
C2= 9495+3*9=9522
Decryption:
M= C2-d*C1
M= 9522-9*3
M=9495
M=HI

It has been verified that the message sent is same as the message that is intended to the destination. The efficiency of the protocol can be increased by adding this specified algorithm.

Analytical Model

In the WSN energy is the most important parameter that has to be analysed. A node has several transmit slots to forward its descendants data, one slot to forward its own data and one slot to broadcast synchronization message to its children. Energy consumption of a node v to transmit is formulated as

$E_t(v)$ = no of cycle * (no of descendants(v)+2) * p_t * t_t

Energy consumption of a node v to receive is formulated as

$E_r(v)$ = no of cycle * (no of descendents(v)+2) * P_r * t_r……. (1)

The decryption procedure of ECC is done in order to increase security and that can be formulated as follows

T_s = C2-d*C1 …….. (2)

As the energy decreases the security should evenly increase so we can say that the energy consumption is inversely proportional to the security associated.

$$E_{usage} \ \alpha \ \frac{1}{T_s} \qquad \ldots\ldots\ldots\ldots\ldots \quad (3)$$

On substituting eq(1) and eq(2) in eq(3) we get

The energy consumption including security can be depicted as follows,

$$E_{usage}(v) = \frac{E_{tx}(v)+E_{rx}(v)+E_{other}(v)}{T_s}$$

$$E_{usage}(v) = \frac{E_{tx}(v)+E_{rx}(v)+E_{other}(v)}{C2-d*C1}$$

Notations

T → Lifetime of a network until first node fails
v → Nodes
T(v) → Lifetime of node
$E_{initial}(v)$ →Available Energy
$E_{usage}(v)$ → Consumption Energy
$E_t(v)$ → Transmit Energy

$E_r(v)$ → Receive Energy
$E_{other}(v)$→ Other causes of energy
p_t → Receiving Power
t_t → Receiving Time
T_s →Decryption
K → Pseudorandom Integer
d→ Private key
r→ Integer value
C1→Cipher text1
C2→Cipher text2
M→Message

Simulation Parameters

In this experiment we are setting different nodes to analyze the performance of the system. Here we consider 30 nodes, we configure the nodes with wireless network properties.

Channel	Wireless channel access
Propagation	Two ray Ground
Physical layer	Wireless physical Layer
MAC Layer	ERMAC
Queue	Droptail
Antenna	Omni-Antenna
Protocol	AODV
Number of nodes	20-30
Simulation Time	1000sec
Simulation Environment	1000*1000
Transmission Range	2Mb/s
Slot Time	9ms
MAC Header	288bits

Evaluation Parameters

The evaluation parameters in this emergency response protocol are as follows:

$$\text{Energy consumption} = \frac{\text{Total energy consumed}}{\text{Total number of nodes}}$$

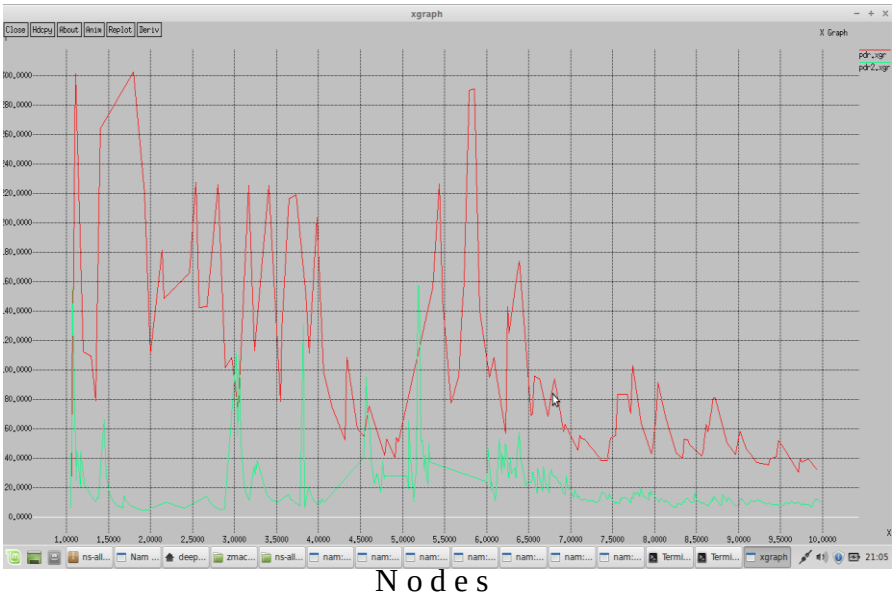
$$\text{Packet delivery ratio} = \frac{\text{num of packets received}}{\text{Total num of packets generated}}$$

$$\text{Latency} = \frac{\text{total time needed by the packet to reach sink}}{\text{Total num of packets received}}$$

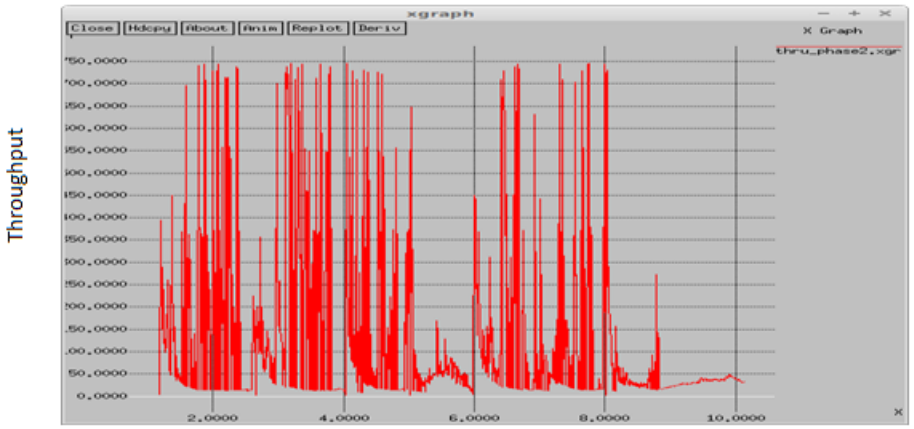
Results

In this way the performance is measured by comparing the existing and proposed and we got that the throughput is greatly increased.

THROUGHPUT

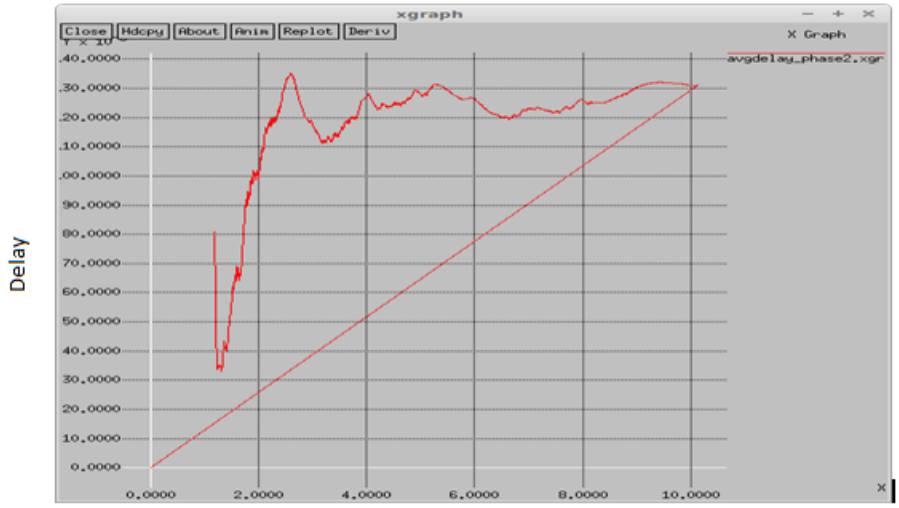


Nodes



Throughput

Nodes



Delay

Nodes

Conclusion

In this paper, Emergency response protocol with network security is proposed which can generate quick responses in an emergency situation such as fire detection and network security is also provided with elliptical curve cryptography in order to prevent n attacker from switching the attacker from normal to emergency monitoring and also to prevent the packets from duplication. By adding ECC algorithm in the proposed protocol efficiency is greatly increased. The future work resides with developing a mechanism that can incorporate the dynamic link estimation.

References

[1] W. Ye, J. Heidemann, D. Estrin, An energy-efficient MAC protocol for wireless sensor networks, in: Proc. 21st Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM'02), 2002, pp.1567–1576.

[2] T. van Dam, K. Langendoen, An adaptive energy-efficient MAC protocol for wireless sensor networks, in: Proc. 1st Int'l Conf. Embedded Networked Sensor Systems (SenSys'03), 2003, pp. 171–180.

[3] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proc. 2nd Int'l Conf. Embedded Networked Sensor Systems (SenSys'04), 2004, pp. 95–107.