ANONYMOUS MULTICAST COMMUNICATION

FOR WIRELESS SENSOR NETWORKS

USING LAYERED ENCRYPTION AND HASHING

A THESIS IN

Computer Science

Presented to the Faculty of the University
of Missouri-Kansas City in partial fulfillment of
the requirements for the degree

MASTER OF SCIENCE

by
JOEL LOPES

B.E. Computer Engineering, University of Mumbai, India, 2007

Kansas City, Missouri
2010

ANONYMOUS MULTICAST COMMUNICATION

FOR WIRELESS SENSOR NETWORKS

USING LAYERED ENCRYPTION AND HASHING

Joel Lopes, Candidate for Master of Science degree

University of Missouri-Kansas City, 2010

ABSTRACT

A sensor network consists of autonomous sensors that operate cooperatively to monitor sensitive information in various environments. A sensor node often sends the information to the base node(s). The base nodes contain the important information, often making them the target of their adversaries. More and more sensor network applications require multicasting to multiple base nodes, and anonymity of the base nodes have become an important aspect of communication in wireless sensor networks. Limited capabilities of the sensor node and a need of multicasting make the issue of anonymity more challenging.

We propose a technique for multiple receiver anonymity. Our solution is based on the layered encryption and hashing for multicasting the data to multiple receivers without compromising the identity of the receiver. We present layered encryption and hashing (LEH) approach for this problem. Our approach uses hash ID to identify as well as randomize a node. Layered encryption provides the confidentiality. Through simulations, we demonstrate that our proposed solution can work efficiently and provide the sink node anonymity for wireless sensor networks.

APPROVAL PAGE

The faculty listed below, appointed by the Dean of the School of Computing and Engineering have examined a thesis titled “Anonymous Multicast Communication for Wireless Sensor Networks using Layered Encryption and Hashing" presented by Joel Lopes, candidate for the Master of Science, and hereby certify that in their opinion it is worthy of acceptance.

Supervisory committee

Baek-Young Choi, Ph.D., Committee Chair
Department of Computer Science and Electrical Engineering

Praveen Rao, Ph.D.
Department of Computer Science and Electrical Engineering

Cory Beard, Ph.D.
Department of Computer Science and Electrical Engineering

CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

Table Page

CHAPTER 1

INTRODUCTION

Wireless Sensor network consists of spatially distributed autonomous sensors network which can serves variety of purposes. The advantage of this type of network is that it can operate autonomously. A sensor node can sense some physical phenomenon and send the information to sink nodes. The path to sink nodes from sensor node can be over a single hop or multi hops.

Most of the existing routing protocols in sensor networks are based on geographic routing in which the sensors have knowledge about their neighbors and location of the sinks. In geographic routing, a sensor usually forwards the packet to the next hop that is closest to the sink sometimes it may consider additional factors like delay and energy consumption.

Variety of application requires a sensor node to multicast information to many sink nodes. For Instance, consider a military application where multiple sensors are deployed in a battle field and soldiers at various base stations are monitoring those sensors. Routing multicast data is mostly based on geographic routing considering important factors like energy consumption, delay, amount of traffic generated etc.

1.1 Motivation

Many wireless sensor network applications require anonymity during their communication. However, there has been little work done on anonymous multicast schemes. Due to inherent differences in the communication, unicast anonymous solutions cannot be directly applied to multicast sensor network. In multicast networks, a receiver needs not only hide itself from sender as in unicast networks but also from other receivers.

When sensor nodes communicate with each other the adversaries can eavesdrop. By analyzing the packet the adversaries can derive the private information. In addition, sinks in a sensor network usually broadcast their addresses before data collection. However, this operation makes sinks vulnerable to attack. Adversaries can attack sinks and obstruct their normal functionality during the step. There may be one or more than one sink nodes in a network. Hiding the identity of these sink nodes is important aspect of the communication, especially because they are more prone to attack. Although there is some work done in anonymous communication and multicast network separately, there is little prior that addresses the problem of multicast anonymization in wireless sensor networks.

1.2 Problem Statement

In this thesis, we propose a solution for an efficient anonymous multicast in a wireless sensor network. Sensor node in WSN has limited memory, energy, and processing capabilities. Hence, a solution should make an efficient use of such resources. Our goal is to protect the privacy of the sink nodes from the active as well as passive attackers.

1.3 Attack Models

Based on attack type adversaries can be broadly divided into active adversaries and passive adversaries. Active adversaries can compromise the security of some nodes and access their memory. Passive adversaries can silently eavesdrop the communication. In this thesis, we assume adversaries can have both type of capabilities.

1.4 Wireless Sensor Node

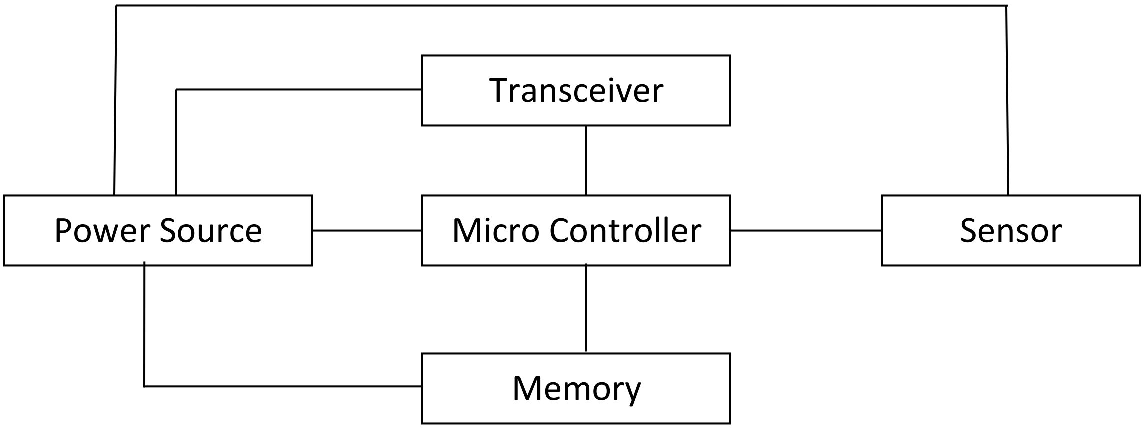


Figure 1: A Wireless sensor node architecture

Figure 1 shows a typical wireless sensor node. Wireless Sensor node consists of following important components

- Power Source

  Power source provides the power for the sensor node. Sensor node can have only limited power source. A good sensor node should consume low energy.

- Micro Controller

  Microcontroller performs tasks, processes data and controls the functionality of other components in the sensor node. Power can be conserved by programming microcontroller to go in sleep state whenever its operation is not required.

- Transceiver

    The functionality of both transmitter and receiver are combined into a single device known as transceivers. . Transceivers lack unique identifiers. The operational states are so called, Transmit, Receive, Idle and Sleep. Various possible options for wireless transmission media are radio frequency, optical communication and infrared.

- Sensor

    Sensor is a hardware device which converts any physical condition into the electronic measure. Sensor senses the physical data of the area being monitored. Characteristics of a good sensor are that it should be small in size, consume low energy, and should be autonomous.

- Memory

    Memory is used to store the data. Flash memory is often used in a sensor node, due to its cost and storage capacity. Memory requirements are very much application dependent. This memory is usually divided into two parts: application memory to store the application and user data, and system memory to store the program and operating system if necessary. This memory may also contain the identification data for the node if necessary.

1.5 Applications

- Green House Monitoring

  Wireless sensor networks may be deployed in the greenhouses to control temperature and humidity. When temperature or humidity falls below the specific level, the manager or in-charge officer must be notified. The exact location or the Identity may need to be hidden from any message which is sent.

- Area Monitoring

  In a battle field type environment, sensor networks are often used to monitor a certain area. When specific event occurs in the area, the event details are sent to the sink node(s). Hiding the location and identity of the sink nodes would be important aspect for this network.

- Machine Integrity Monitoring

  Wireless sensors can be installed in the commercial airplanes or navy ships to monitor the health of the various parts of engine and the base station as well on system installation monitor the integrity of these parts.

CHAPTER 2

BACKGROUND WORK

2.1 Anonymity

There have been anonymity techniques proposed for wired and wireless networks, and multicast/unicast communications. Usually techniques for wired network anonymity cannot be applied to wireless network and vice versa due to the medium and the forwarding type. Table 1 compares the previous work done in this field. Among them, RRHA [3] and XOR tree [6] do support the multicast and wireless network. However, XOR tree technique is infeasible due to excessive synchronized key sharing [14], and RRHA is generates lot of traffic as it is based on flooding.

Table 1: Comparison of previous anonymous communication techniques

	Method for Anonymity	Multicast	Wireless
Mutual anonymous multicast(MAM) [2]	Encryption	Yes	No
Randomized routing with hidden address (RRHA) [3]	Broadcast	Yes	Yes
Reverse onion ring protocol [4]	Encryption	No	Yes
M2 [5]	Encryption	Yes	No
XOR-Trees for efficient Anonymous Multicast and Reception [6]	Encryption	Yes	Yes
Hashing Based ID Randomization(HIR) [7]	Encryption+ Randomization	No	Yes

2.2 Mutual Anonymous Multicast (MAM)

MAM [2] creates the overlay network for the anonymous unicast communication and the central server for the anonymous multicast. Nodes in

MAM are divided into anonymous member nodes (AM), non-anonymous member nodes (NM) and middle outsiders (MO) based on a trust level.

A set of NM nodes form a multicast tree. AM nodes connect the unsaturated NM nodes using unicast anonymity protocol. MO nodes are later invited to improve to cost efficiency of tree. Once tree is created, an encryption based approach is used to communicate anonymously.

2.3 Randomized Routing with Hidden Address (RRHA)

RRHA [3] system sends symmetric encrypted data over a network in predefined number of paths. Every node on the path tries to identify if the data is intended for that node. Otherwise, it decrements the hop count and forward the packet. This process is continued until packet reaches to a final destination or the hop count reaches zero. By increasing the number of packets, the probability destination receiving packet can be increased. Figure below illustrates this operation.

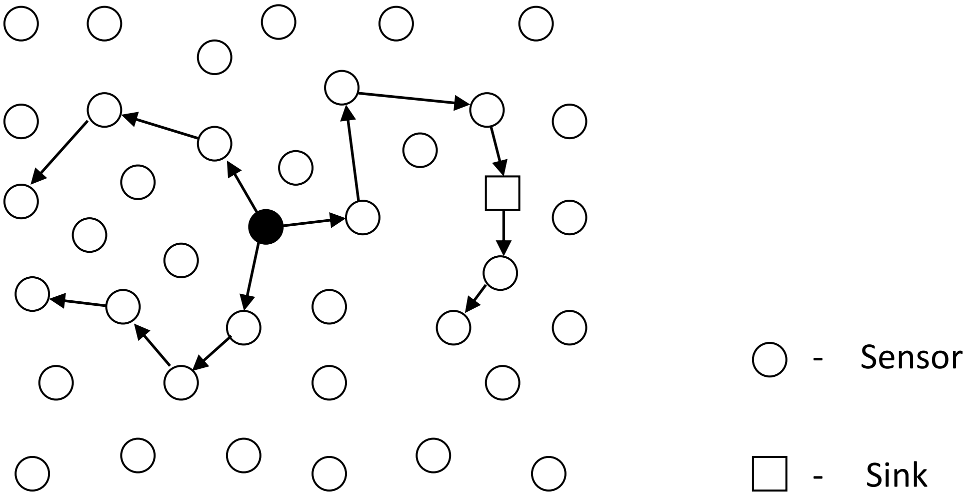


Figure 2: RRHA with multiple paths. Source node forwards packet to three different random paths.

Since direction of packets is not used in this technique, a packet may come back to the source. In addition, there is no way to know if a destination has received the packet.

2.4 Reverse Onion Ring Protocol [4]

This technique emphasizes on the creation of ring for a communication, and the onion ring protocol is used to gather the request from the other nodes in the ring. Various layered of routing can also be performed based on a trust level between nodes.

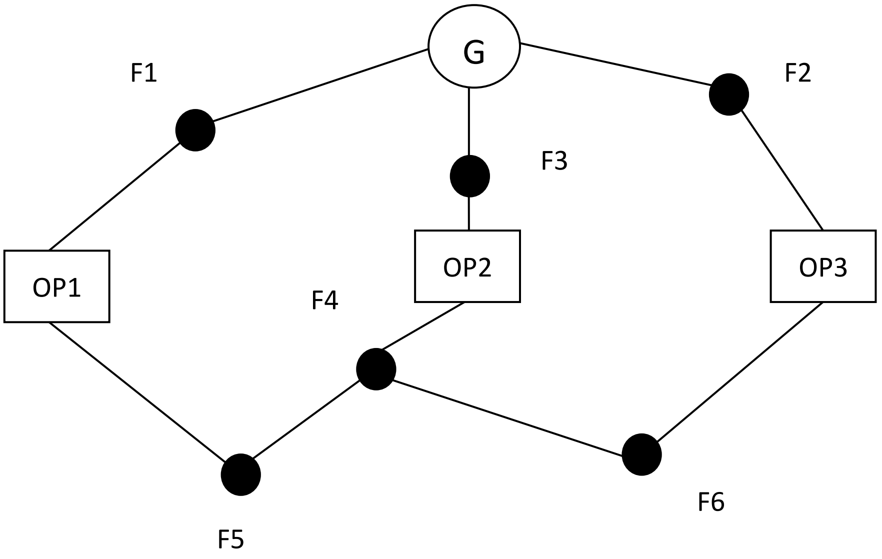


Figure 3: Reverse onion ring protocol

Figure 3 shows the typical network setup for reverse onion ring protocol. G trusts OP1, OP2 and OP3. G forms several rings say G, OP1, OP2 and G, OP1, OP3. G then sends packet to OP1 and OP2 using onion ring. OP1 decrypts the packet and add F5 and F4 along its path using onion ring. If F5 and F4 have any data to send then it will encrypt data and send it along with packet otherwise it will decrypt packet and forward it to next hop.

This solution cannot be applied directly to a multicast network, as it is difficult to create ring in a multicast network. Also this approach is based on trust level which is difficult to maintain in the wireless environment.

2.5 M2

M2 [5] uses a mix network along with the tree structure to achieve multicast anonymity. Each consumer registers individually with the content producer by sending a registration message through mix network, though a mix on path might merge this registration into previous registration by a member of the same group. As we get more registration messages, a multicast tree is formed by merging registrations. Figure 4 illustrates this operation.

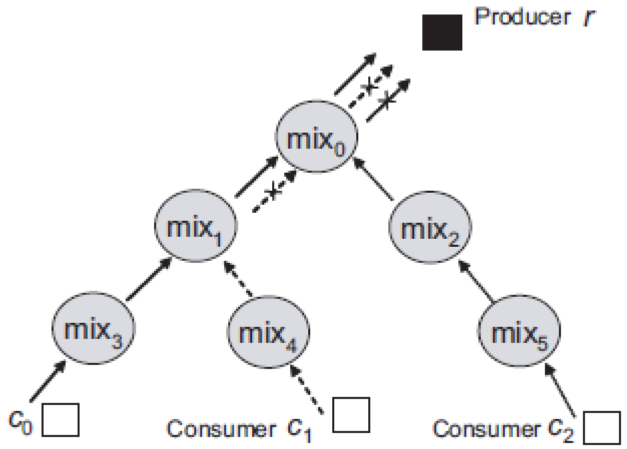


Figure 4: M2: Merging registration paths

Once a multicast tree is formed, we use Mix processing to multicast packet from producer to consumer.

Since each packet follows the same path, pattern attacker can identify the destination node as well as participating nodes by analyzing the traffic.

2.6 Hashing Based ID Randomization

HIR [7] proposed a hashing based technique for ID randomization. Every node in a network uses chain hashing to create its ID which is used for communication. Hashing key is changed on a periodic interval so that the compromise in the hash key can be overcome. However, it involves lot of calculation on nodes, and more storage space, an overhead of periodic key exchange.

2.7 Secure Anonymous Routing [8]

Secure Anonymous routing proposed is based on encryption and certificate exchange for an anonymous communication. This approach uses mobile routers with high speed wireless backbone that hides the mobile client from outside networks. This approach doesn’t support multicast. Also, mobile routers can become a bottleneck in such networks, as it is not totally distributed.

CHAPTER 3

LAYERED ENCRYPTION PROTOCOL

Layered encryption is a technique for anonymous communication over a computer network. The main idea behind the layered encryption is to protect the privacy and identity of sender as well as receiver.

Messages are encrypted and send over number of nodes. Each node removes a layer of encryption understand the next node on the path and forward message to the next router on the path. Therefore the routing node is only aware of the previous and next node on its path.

Routing node is unaware of the source or final destination of the message. Also the incoming and outgoing data at each node are different for any given packet as decryption takes place at each node. This provides strong degree of unlinkability.

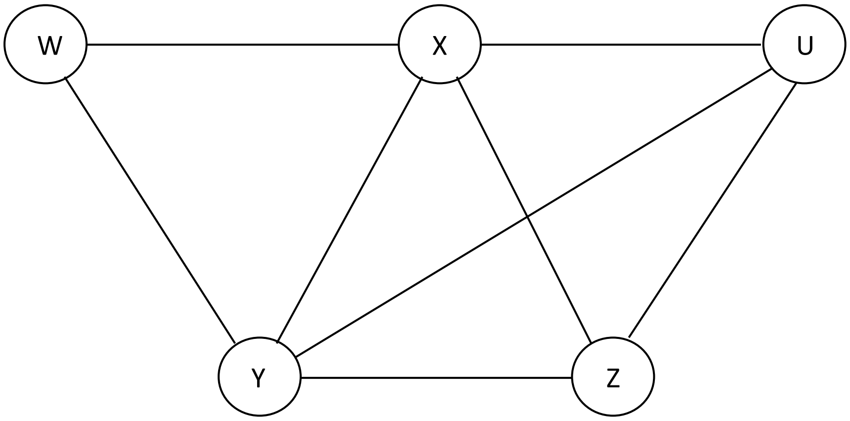


Figure 5: A sample network for layered routing

Suppose in network shown in figure 5 W wants to send data to Z. process for layered encryption communication would be as follow.

- W will choose random path to Z (Say, W->X ->Y->Z)

- Then W will encrypt the message with the key for all intermediate nodes in path E(X,E(Y,E(Z,data)))

- At each node packet is decrypted and forwarded to next intermediate node

- Ultimately packet reaches destination

At each node single encryption is removed like peeling an onion at each node, hence it is called a layered encryption. When a packet is received, each node knows who sends the packet and whom to forward the packet. However, it has no idea about the number of nodes in a packet and communication initiator or receiver.

3.1 Advantages

- Paths are unpredictable
- Incoming and outgoing messages at each router are different i.e. Strong degree of unlinkalibility.
- If one or two onion router compromise, still anonymity can be achieved

3.2 Drawbacks

Intersection attacks rely on the fact that node periodically fail or leave the network; thus, any communication path that remains functioning cannot have been routed through those routers that left, neither can it involve routers that joined the network recently.

In a predecessor attack, an attacker who controls a node keeps track of a session as it occurs over multiple path reformations (paths are periodically torn down and rebuilt). If an attacker observes the same session over enough reformations, it will tend to see the first router in the chain more frequently than any other routers.

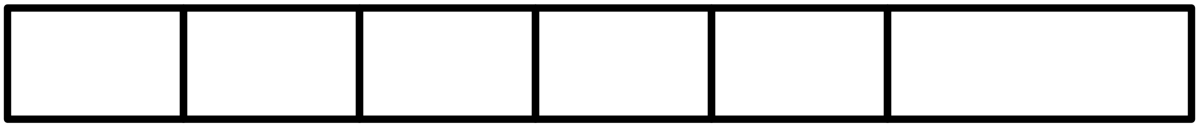
CHAPTER 4

LAYERED ENCRYPTION AND HASHING (LEH) TECHNIQUE

In this chapter, we discuss the proposed LEH technique. We first remark the packet format. We then explain how the multicast tree is created. Finally, we describe LEH for wireless anonymous communication.

4.1 Packet Format

Every packet transferred using LEH is an encrypted packet containing the destination Id, number of next paths and packet for each path. Figure below shows the general packet structure.



Where H_X – Hash ID of receiving Node

N - Number of different routes

E_{Ri} - Encrypted route i

The above packet would be encrypted with a symmetric shared key for X and transmitted. Here N denotes the total number of sub packets in this packet. X here will decrypt the packet to separate E_{Ri} (i=1,…,n) and forward packet to each E_{Ri} along with data.

4.2 Creating Multicast Tree

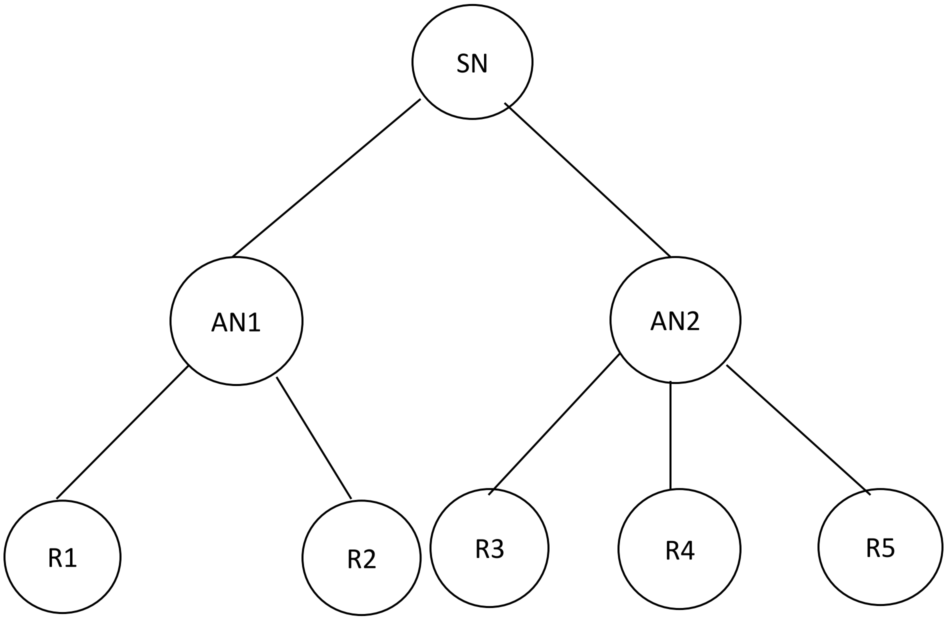


Figure 6: Multicast tree

A receiver here knows the id of the sensor node from which it wants to receive data. The receiver first broadcasts the discover packet encrypted with the public key for authority node. Intermediate authority nodes decrypt the packet. An authority node creates the reply packet containing its own id and broadcast it.

A receiver selects an authority node and reply back to the authority node. The authority node then adds the receiver to its own database.

The algorithm for a registration process for any node with an authority node is as shown below.

```
Algorithm: Node Register
If Packet Type= Discovery
If (SID is in my database) then
        Extract the node id
        Create and Send back the data available onion to the node
    Else
        Decrement hop count and forward packet
    End If
End If
IF (Packet type= Register) then
    Insert the node ID, Sensor ID into database
End If
```

4.3 Layered Encryption Multicast

For this approach, we use the layered encryption protocol for a multicast that includes all the paths to receivers.

4.3.1 Create Data Packet

We first create the data packet using layered encryption for each path on the multicast tree, and then broadcast the data packet. The algorithm is shown below.

Algorithm for creating data packet

```
Algorithm: Create Packet
For Each node registered with the sensor ID
    Create data packet for receiver(s)
    Forward Packet
End For
Create some null packet and forward it to random nodes
```

4.3.2 Received Packet Processing

If the node is not the authority node, then it will decrypt the packet and forward it to the next node. If node is authority node, then it will decrypt packet, and follow create data packet algorithm for next path(s). If node is sink node, then it will decrypt the data, and forward some dummy packets.

4.3.2 A Remark

Even though this approach provides good anonymity, it lacks in the efficiency. The number of encryption and decryption for this approach is greater which makes it less efficient.

4.4 Layered Encryption and Hashing

In the previous approach, we achieve anonymous multicast by multiple anonymous unicast. Since it is not exploiting the nature of multicast, it was not as efficient as it can be. To address the issue, we create a routing tree and encrypt the packet for the entire tree. Each packet is routed using different tree.

We select a random path from the source to one of the destinations. We then calculate optimal paths to other nodes. Once paths for all destinations are selected, we create a tree for all paths, and encrypt the tree level to create a data packet. This data packet is transmitted over a network to a next node on the path. Every node in the tree that receives a packet decrypts it, divides the packet if necessary, and forwards it to next node(s) in the tree.

When an authority node receives this data packet, it decrypts the data and follows same procedure to forward data to next authority node/sink node. When a sink node receives a packet, it simply decrypts the packet and sends a dummy packet.

4.4.1 Creating Data Packet

To create a data packet, a sensor node selects a random path to one of its destination nodes. Then, for each node on path, it calculates the shortest path to the other node, and selects the optimal one. Once such paths are selected, we create a tree using those paths. This tree is then encrypted level by level starting from the leaf nodes till the root node. This entire packet is then transmitted over the network to the next nodes on the path.

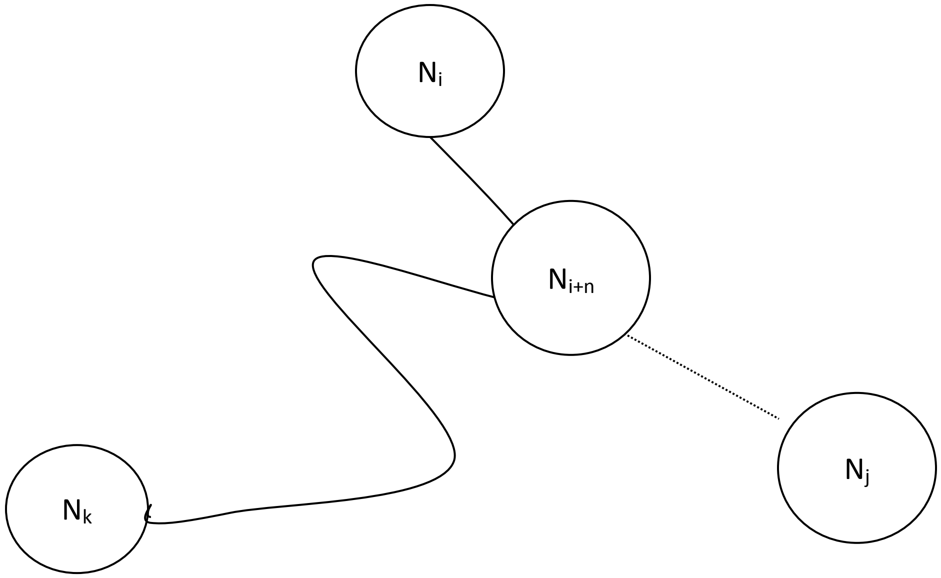


Figure 7: Path merging for anonymous communication

Creating path(s) : First, select a random path from N_i to N_k and denote it as P_i. Next, find a nearest node for N_j from Pi, say N_{i+n}, so path P_{i+1} would be N_i->N_{i+n}->N_j. Repeat for all nodes in the table $T_{j.}$ For all nodes that share common nodes, merge those paths to create a tree. Figure 8 shows a typical tree from paths P_i,P_{i+1}, ….

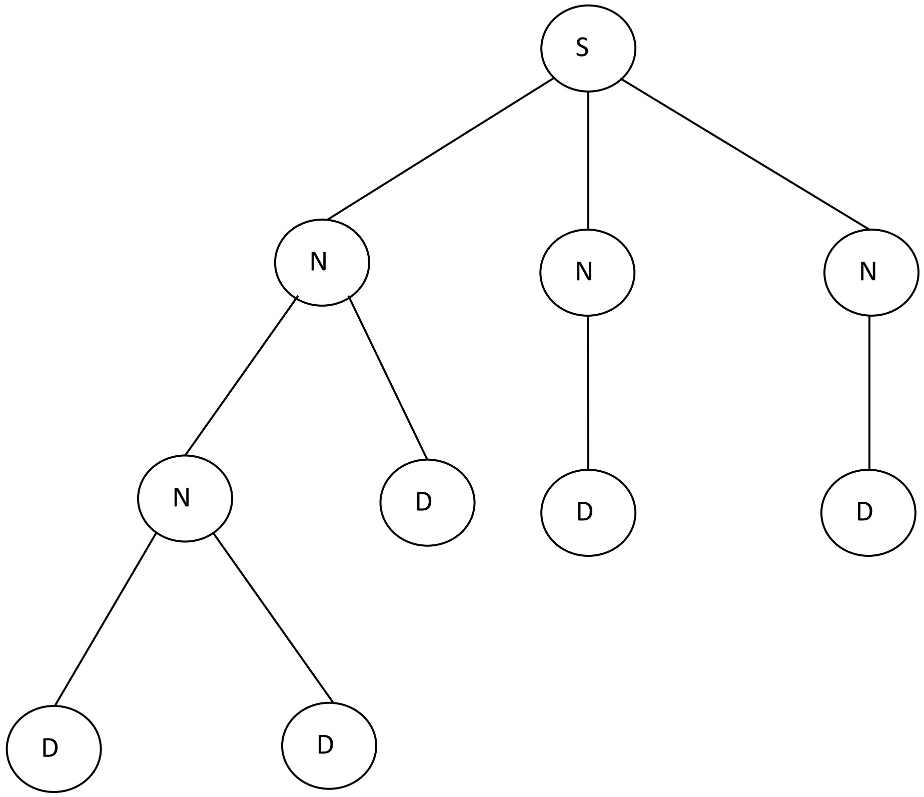


Figure 8: Multicast tree showing various paths

Encrypt the hash if of leaf node so we have $E_{D1}(H_{D1})$, $E_{D2}(H_{D2})$, $E_{D3}(H_{D3})$, $E_{D4}(H_{D4})$, $E_{D5}(H_{D5})$. Combine the data of all child nodes and encrypt the data again so data at N2 would be $E_{N2}(E_{D1}(H_{D1})||E_{D2}(H_{D2}))$. Therefore, the final data would be $E_{S1}(E_{N1}(E_{N2}(E_{D1}(E_{D1})||E_{D2}(E_{D2}))||E_{D3}(H_{D3}))||E_{N3}(E_{D4}(H_{D4}))||E_{N4}(E_{D5}(H_{D5})))$.

Algorithm: Create Data Packet

```
Step 1: Create multicast tree for all registered receivers
Step 2: Get the depth of tree
Step 3: For i=depth to 0 continue
            If node j at depth i has child nodes($X_l$,…,$X_k$)
            then
                set N=number of child nodes
                $H_{j,}E(N,X_l,\dots,X_k)$
            Else
                $H_{j,}E(H_j)$
```

4.4.2 Received Packet Processing

A receiving node tries to decrypt the packet verify if the particular node is receiver with the destination ID field. If the receiving node successfully decrypts the received packet, then it divides packet into the number of paths, and forwards each packet on different paths.

If a current node is the authority node, then create a new data packet using above procedure for next authority nodes/sink nodes.

CHAPTER 5

ANONYMITY AND ATTACK ANALYSIS

In this section, we analyze the anonymity and security of our system against adversaries. Attacks can be either active attack or as passive attacks.

5.1 Anonymity Analysis

All packets that are transferred between our communications are encrypted. During multicast tree creation process asymmetric encryption process is used for security and later symmetric encryption is used for faster security. Hence, adversaries can't determine neither the content of packet nor the destination of any packet.

Compromised routing nodes can't derive any information from the received packet as the content of packet is encrypted. This technique will also protect attack of analyzing amount of incoming and outgoing traffic as different paths are used for each packet.

5.2 Attack Analysis

Because of open communication medium and multi-hop characteristic sensor nodes are prone to active as well as passive attacks. Passive attack could tamper confidentiality of system, whereas active attack could harm the operation of the entire system. Listed below are some security features of the proposed system.

- Falsification

  In this type of attack, we assume attacker can alter the data and broadcast the packet. All packets that are communicated on network are encrypted via various layers. We also have the hash key for each data packet to validate the integrity of the packet.

- Identity spoofing

  Adversaries communicate using identity of the other node. All communications are encrypted via a shared session key. For identity spoofing, adversaries should know the shared symmetric key for each node on the route.

- Man In middle attack

  In this attack, adversaries palace itself between two communicating nodes and analyze the communication between them. If adversaries are the part of the routing path, then it can only decrypt one layer of data. It cannot interpret what would be decrypted data after next layer. If adversaries are not part of the routing path, then it cannot affect the communication and cannot derive any information form data received.

- Eavesdropping

  Attacker can silently listen to the communication in the network. Incoming and outgoing message at each node would be different as incoming message is encrypted and outgoing is decrypted. Therefore, there is strong degree of unlinkability between incoming and outgoing messages. Also the entire communication is encrypted, as we stated before.

- Sniffer Attack

  A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. As our communication is encrypted sniffer attack won't affect out system.

CHAPTER 6

PERFORMANCE EVALUATION

In this chapter, we first provide the details for our simulation setup. We then evaluate the performance for onion ring multicast routing, and anonymous multicast path routing. For the performance evaluation of the proposed, we have used OMNET++ simulator [17]. The evaluation is done for single sensor-multiple receivers. The field size is fixed for the evaluation purpose.

The various performance metrics used are:

- Packet size overhead: It is the additional headers for the encryption/decryption information. This Information is the total of the entire header for all receivers for single packet delivery.

- Average packet delivery time: This is the elapsed time until the last node receives its data.

- Energy: It is the sum of all energy used for a single packet delivery.

- Network lifetime: It is the time elapsed until a first node goes down.

6.1 Experimental Setup

Sensor Node

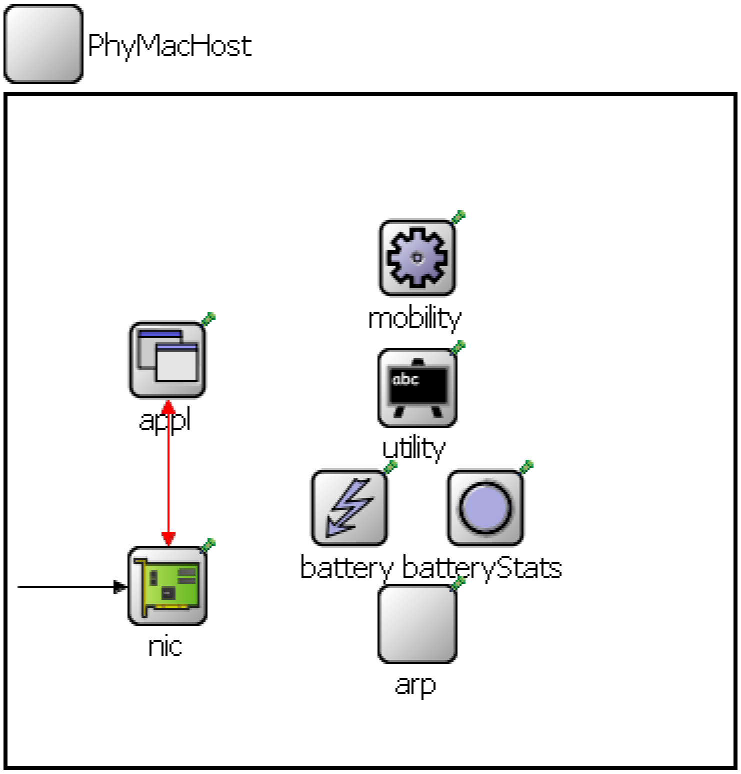


Figure 9: Model sensor node for simulation

Figure 9 shows the sensor node implemented for our experimental setup.

Different components of the node are:

- Appl – This module is an application layer implementation for the node. This layer handles the packet creation, encryption, decryption and forwarding decisions.
- NIC - This module is the NIC implementation using transceiver settings from Texas Instrument CC2420.
- ARP - ARP module is used by node to obtain its dynamic address.
- Battery – Battery modules initializes itself with initial power and manages the power distribution across the node.
- Battery Stats- Battery Stats handles and maintains the stats for the battery module.
- Mobility- Mobility module is used for setting the initial position for node and then the mobility parameters. For our simulation only initial position is used mobility parameters are set to none. Since our work concentrates on the stationary sensor network.
- Utility- Utility has the various utility modules.

Figure 10 shows the NIC card for our simulation

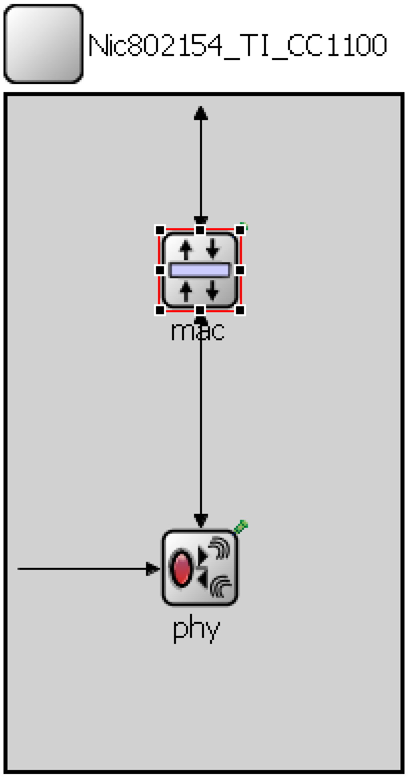


Figure 10: Model NIC

- Average packet delivery time

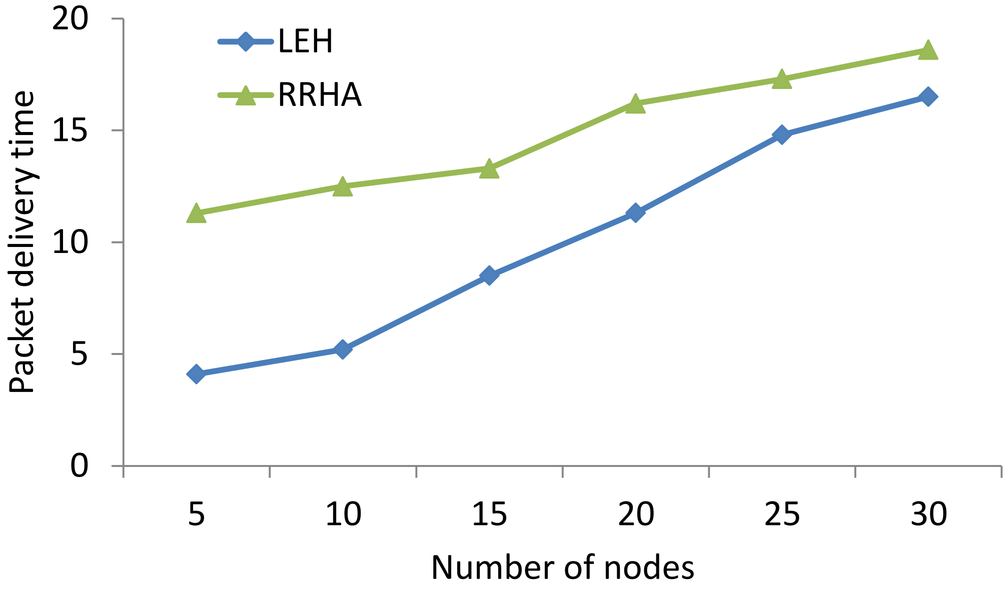


Figure 11: Average packet delivery time

Figure 11 shows the average packet delivery time for Layered encryption and hashing and Randomized routing with hashing by varying number of nodes. LEH sends data to selected number of nodes and RRHA floods data to all its neighbors which results in more collision and retransmission. Hence LEH sends data faster. Therefore LEH performs better as compared to RRHA in terms of packet delivery time.

- Overhead analysis

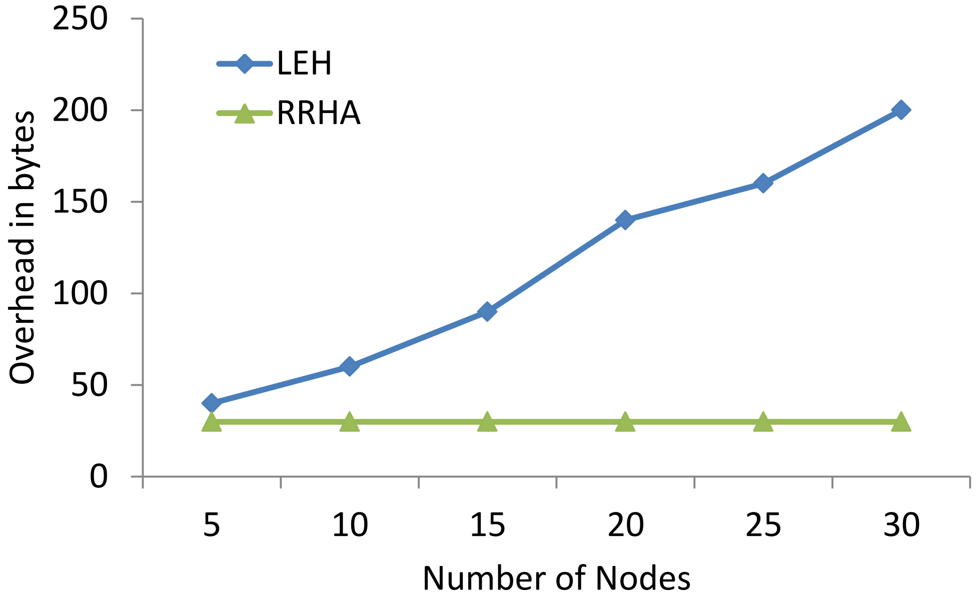


Figure 12: Overhead analysis

Figure 12 shows the overhead analysis in terms of the additional data attached per packet for encryption, decryption and hashing for LEH and encryption, decryption for RRHA. LEH has layered encryption hence more encryption, decryption is performed as number of nodes increases whereas RRHA has end to end decryption hence almost constant overhead irrespective of the number of nodes. This phenomenon is evident from the figure 12.

- Total energy consumption per packet

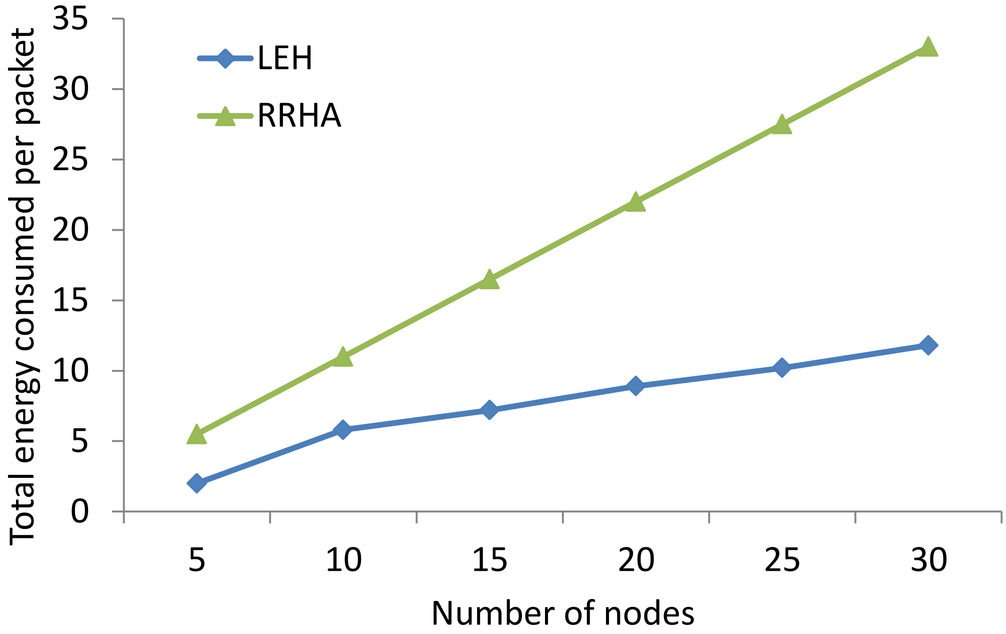


Figure 13: Total energy consumption

Total energy consumption is calculated by summing up all the receiving and transmission power of all nodes participating in communication of one packet from a source to destinations. The processing energy is ignored for this evaluation purpose. With LEH, we have controlled the number of nodes participating in a communication, hence not all nodes participate in the communication of a single packet. As a result, we have less energy consumption per packet transmission as compared to RRHA.

- Network Lifetime

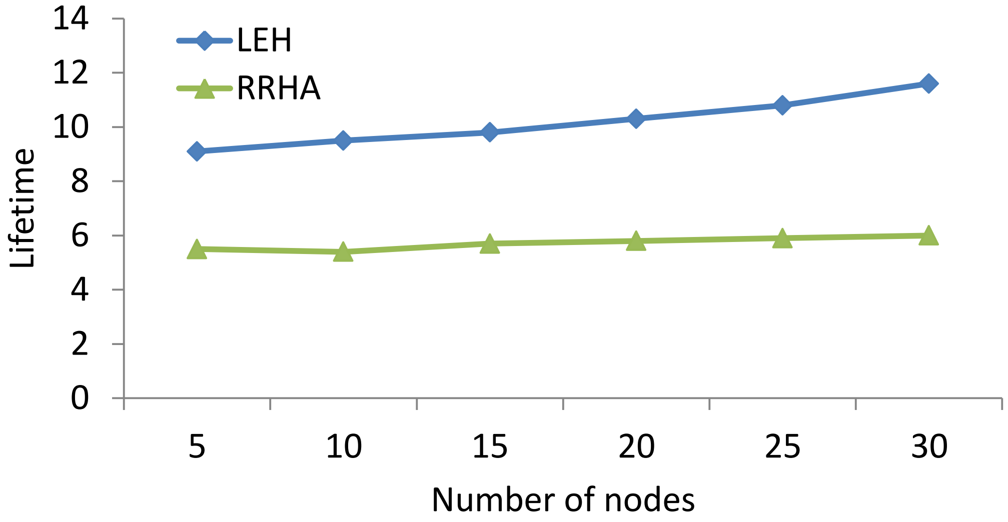


Figure 14: Network lifetime

Network life time is calculated as the time elapsed until a first node goes down due to energy depletion. In RRHA, all nodes forward a packet, whereas in LEH, only selected nodes forward packet that provided extended lifetime. Therefore, LEH outperforms RRHA, as can be seen in Figure 14.

CHAPTER 7

CONCLUSION AND FUTURE RESEARCH

In this thesis, we addressed the problem of multicast anonymity for wireless sensor networks, using layered encryption and hashing. Layered encryption allows anonymity of receiving nodes, and hashing provides randomization. We evaluated the performance of our approach by comparing to RRHA approach using OMNET++ simulations.

Our approach provides the receiver anonymity achieving the sender as well as receiver anonymity for wireless sensor networks would be interesting study. Study of our approach by varying density of sensor nodes would be of interest in future.

REFERENCES

1 Brown, Zach. Cebolla - Pragmatic IP Anonymity. In *Ottowa Linux Symposium* (Ottawa, Ontario 2002), 55-59.

2 Xiao, Li, Liu, Xiaomei, Gu, Wenjun, Xuan, Dong, and Liu, Yunhao. A design of overlay anonymous multicast protocol. In *Proceedings of the IPDPS* (Rhodes Island 2006), IEEE Computer Society, 25-29.

3 C, Edith and Ngai, -H. On providing sink anonymity for sensor networks. In *International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly* (Leipzig, Germany 2009), ACM, 269-273.

4 Li, Ru, Pang, Liaojun, Pei, Qingqi, and Xiao, Guozhen. Anonymous Communication in Wireless Mesh Network. In *Proceedings of the 2009 International Conference on Computational Intelligence and Security* (Beijing 2009), IEEE Computer Society, 416-420.

5 Perng, Ginger, Reiter, Michael K., and Chenxi, Wang. M2: Multicasting Mixes for Efficient and Anonymous Communication. In *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems* (Lisboa, Portugal 2006), IEEE Computer Society, 59-59.

6 Dolev, Shlomi and Ostrovsky, Rafail. Xor-Trees for Efficient Anonymous Multicast and Reception. *ACM Transactions on Information and System Security* , 3, 2 (May 2000), 63-84.

7 Yi, Ouyang, Zhengyi, Le, Yurong, Xu, Triandopoulos, N, Sheng, Zhang, Ford, J., and Makedon, F. Providing Anonymity in Wireless Sensor Networks. In *IEEE International Conference on Pervasive Services* (Istanbul 2007), IEEE Computer Society, 145-148.

8 Xiangfang, Li, Lijun, Qian, and Kamto, J. Secure Anonymous Routing in Wireless Mesh Networks. In *International Conference on E-Business and Information System Security* (Wuhan 2009), 1-5.

9 Goldschlag, David, Reed, Michael, and Syverson, Paul. Hiding Routing Information. In *Proceedings of the First International Workshop on Information Hiding* (Cambridge May 1996), Springer-Verlag, 137-150.

10 Kelly, Douglas, Raines, Richard, Baldwin, Rusty, Mullins, Barry, and Grimaila, Michael. Towards a Taxonomy of Wired and Wireless Anonymous Networks. In *Proceedings of the 2009 IEEE international conference on Communications (ICC'09)* (Dresden, Germany 2009), IEEE Press, 585-592.

11 Song, Sejun, Choi, Baek-Young, and Kim, Daehee. MR. BIN: Multicast Routing with Branch Information Nodes for Wireless Sensor Networks. In *Proceedings of 19th International Conference on Computer Communications and Networks (ICCCN)* (Zurich August 2010), IEEE Computer Society, 1-6.

12 Tian He Stankovic, J.A. and Chenyang Lu Abdelzaher, T. SPEED: a stateless protocol for real-time communication in sensor networks. In *23rd International Conference on Distributed Computing Systems, 2003.* (Providence, Rhode Island 2003), IEEE Computer Society, 46-55.

13 Jalil, K.A. and Nategh, M.H. A composed energy aware metric for WSNs. In *2010 International Conference on Computer Design and Applications (ICCDA)* (Qinhuangdao 2010), IEEE Computer Society, 558-561.

14 Boukerche, A, El-Khatib, K, Li , Xu, and Korba, L. SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. In *29th Annual IEEE International Conference on Local Computer Networks, 2004.* (Tampa, Florida 2004), IEEE Computer Society, 618-624.

15 Sherwood, Rob , Bhattacharjee, Bobby , and Srinivasan, Aravind. P5: A Protocol for Scalable Anonymous Communication. In *IEEE Symposium on Security and Privacy, 2002.* (Berkeley, California May 2002), IEEE Computer Society, 58.

16 Jung-Chun, Kao and Marculescu, R. Energy-efficient anonymous multicast in mobile ad-hoc networks. In *2007 International Conference on Parallel and Distributed Systems* (Hsinchu 2007), IEEE Computer Society, 1 - 8.

17 Omnet++ V4.1, http://www.omentpp.org.

VITA

Joel Lopes was born in 1st October 1985 in Mumbai, India. As a High school student he was interested in Math and Science. He graduated from high school in 2001. With deep interest in computer science and technology Joel gained in Diploma in computer technology in 2004. With desire to learn more about computer he joined University of Mumbai for Bachelors in Computer Engineering. He graduated from University of Mumbai in 2007. After working as an Assistant Software Engineer in Tata Consultancy Services for a year Joel began his Master’s program in Computer Science. While pursuing his master’s degree he worked as a Graduate Research Assistant in Database and Information systems laboratory. He also worked as a Graduate Assistant and has done 8 months internship at Open Methods. After Completion of his degree Joel plans to pursue challenging carrier as a Software Developer.