International Journal of Research in Advent Technology, Vol.3, No.4, April 2015
E-ISSN: 2321-9637

WSN for Industrial Applications using PSR based Energy Routing (zigbee)

Sivasakthiselvan.S[1], Prabu.R[2], Vinothkumar.S[3]
[1]*PG Scholar,* [2]*Assistant Professor,*[3]*Associate Professor*
[1,2,3]*Department of Electronics and Communication Engineering*
Aksheyaa College of Engineering, Pulidivakkam, Kanchipuram-603 314, Tamilnadu, India
mangaivasan@gmail.com

***Abstract*—** Wireless Sensor Networks (WSNs) are used for various applications such as habitat monitoring, automation, agriculture, and security. Wireless sensor network consists of large number of small nodes. The measurement of temperature & light by the use of sensors in which there are different nodes/motes placed at different locations. These nodes are having different node identification & they will sense the temperature & light of their surrounding location and send it to the base station node. The main aim of this project is to detect the failure node and network nodes are route based on the Active node by Power Management Principle and then prevent unauthorized access of wireless data from spoofed using Zigbee technology. The identity of a node can be verified and then access. In this project, I propose to use spatial information, a physical property associated with each node, hard to falsify, as the basis for 1) Detecting the failure nodes 2) Monitoring the active node power and sensed data, then network nodes are activated depends upon the power level of the active node. Nodes in a sensor network are severely constrained by energy, storage capacity and computing power. To prolong the lifetime of the sensor nodes, designing efficient routing protocols is critical 3) detecting spoofing attacks the proposed model can be explored further to improve the accuracy of determining the distance between one node to another nodes by use of spatial correlation of received signal strength (RSS) inherited from wireless nodes to route the information for next nearest node.

Index Terms—Proactive Source Routing (PSR), Failure node detection, Breadth First Search(BFST) Algorithm, master and slave nodes, Alternate path finding, Neighbor path information, Energy based Routing, Alternative node activity.

1. INTRODUCTION

A sensor network is designed to perform a set of high-level information processing tasks such as detection, tracking, or classification. Measures of performance for these tasks are well defined, including detection of false alarms or misses, classification errors, and track quality. Applications of sensor networks are wide ranging and can vary significantly in application requirements, mode of deployment (e.g., ad hoc versus instrumented environment), sensing modality, or means of power supply (e.g. battery versus wall socket).

Sensor networks extend the existing Internet deep into the physical environment. The resulting new network is orders of magnitude more expansive and dynamic than the current TCP/IP networks and is creating entirely new types of traffic that are quite different from what one finds on the Internet now. Information collected by and transmitted on a sensor network describes conditions of physical environments for example, temperature, humidity, or vibration and requires advanced query interfaces and search engines to effectively support user-level functions. Sensor networks may inter-network with an IP core network via a number of gateways. A gateway routes user queries or commands to appropriate nodes in a sensor network. It also routes sensor data, at times aggregated and summarized, to users who have requested it or are expected to utilize the information. A data repository or storage service may be present at the gateway, in addition to data logging at each sensor. The repository may serve as an intermediary between users and sensors, providing a persistent data storage. It is well known that communicating 1 bit over the wireless medium at short ranges consumes far more energy than processing that bit.

In all previous methods, they cannot be use sensor node failure detection before the data transferring and receiving, then if the node is failing immediately alternate path will be fined for data communication by using the Breadth First Search Tree (BFST) algorithm. If the node is failure condition automatically that will be sent the alert the next nearest neighbor node by using Destination Sequence Distance Vector (DSDV) routing protocol.

2. RELATED WORK

Z. E. Perkins and P. Bhagwat[1]The basic idea of the design is to operate each Mobile Host as a specialized router which periodically advertises its view of the interconnection topology with other Mobile Hosts within the network. This amounts to a new sort of routing protocol. We have investigated

modifications to the basic Bellman Ford routing mechanisms as specified by RIP to make it suitable for a dynamic and self-starting network mechanism as is required by users wishing to utilize ad hoc networks. Our modifications address some of the previous objections to the use of Bellman Ford related to the poor looping properties of such algorithms in the face of broken links and the resulting time dependent nature of the interconnection topology describing the links between the Mobile Hosts. Finally we describe the ways in which the basic network layer routing can be modified to provide MAC layer support for ad hoc networks.

R. Rajaraman[2]described anticipate that due to the advent of peer-to-peer computing, the two problem domains will bear an even stronger relationship; peer-to-peer networks share many of the same concerns with ad-hoc networks, e.g., a need to quickly adapt to the frequent changes in the system and completely decentralized organization. An interesting direction for future research is to see whether resource location protocols designed for peer-to-peer networks can be adapted to yield effective routing protocols for ad hoc networks.

S. Biswas and R. Morris[3]describes ExOR, an integrated routing and MAC protocol that increases the throughput of large unicast transfers in multi-hop wireless networks. ExOR chooses each hop of a packet's route after the transmission for that hop, so that the choice can reflect which intermediate nodes actually received the transmission. For pairs between which traditional routing uses one or two hops, ExOR's robust acknowledgments prevent unnecessary retransmissions, increasing throughput by nearly 35%. For more distant pairs, ExOR takes advantage of the choice of forwarders to provide throughput gains of a factor of two to four.

Z. Wang[4] proposed tackle the problem of opportunistic data transfer in mobile ad hoc networks. Our solution is called Cooperative Opportunistic Routing in Mobile Ad hoc Networks (CORMAN). It is a pure network layer scheme that can be built atop off-the-shelf wireless networking equipment. Nodes in the network use a lightweight proactive source routing protocol to determine a list of intermediate nodes that the data packets should follow en route to the destination. Here, when a data packet is broadcast by an upstream node and has happened to be received by a downstream node further along the route, it continues its way from there and thus will arrive at the destination node sooner. This is achieved through cooperative data communication at the link and network layers. This work is a powerful extension to the pioneering work of ExOR. We test CORMAN and compare it to AODV, and observe significant performance improvement in varying mobile settings.

To overcome the problems in the traditional techniques, this paper proposes can be use sensor node failure detection before the data transferring and receiving, then if the node is failing immediately alternate path will be fined for data communication by using the Breadth First Search Tree (BFST) algorithm. If the node is failure condition automatically that will be sent the alert the next nearest neighbor node by using RSS (Received Signal Strength) then depends upon the power level of the active node in the network.

3. PROACTIVE SOURCE ROUTING IN WSN

Traditional each node in the network has routing table for the broadcast of the data packets and want to establish connection to other nodes in the network. These nodes record for all the presented destinations, number of hops required to arrive at each destination in the routing table. The routing entry is tagged with a sequence number which is created by the destination node. To retain the stability, each station broadcasts and modifies its routing table from time to time. How many hops are required to arrive that particular node and which stations are accessible is result of broadcasting of packets between nodes. Each node that broadcasts data will contain its new sequence number and for each new route, node contains the following information:

– How many hops are required to arrive that particular destination node.

– Generation of new sequence number marked by the destination.

– The destination address.

The proactive protocols are appropriate for less number of nodes in networks, as they need to update node entries for each and every node in the routing table of every node. It results more Routing overhead problem. There is consumption of more bandwidth in routing table. Example of Proactive Routing Protocol is Destination Sequenced Distance Vector (DSDV).

4. DESCRIPTION OF THE PROPOSED SYSTEM

In our Proposed System we can use three modules that is Monitoring module, Coordinator or Controller module and End Device module.

Monitoring Module:

We can be use for Monitoring purpose from the coordinator of controller node by using the UART port to the Personal computer. It is used for displaying the End device information like node current, voltage and power and also displayed which node is active condition and standby condition or turn off condition.

Coordinator or Controller Node:

It is used for coordinating all nodes for the data communication.

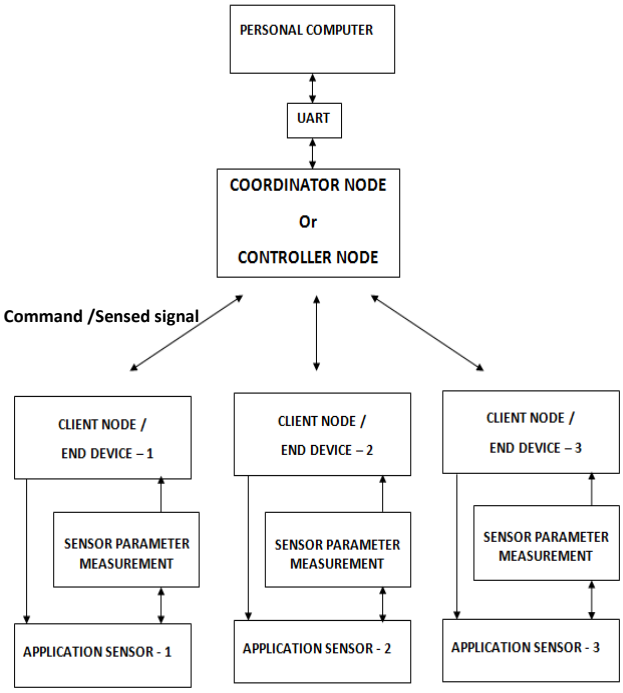

Fig.1 Functional Block Diagram

Collecting the information about the end device through the broadcast if any node failure in the network that will be eliminated and choose the alternative paths for data communication. It operates full duplex mode that means the control signal will be send to the client or end nodes, at the same time sense the condition of the application sensor from the end device.

End Device:

It is used for connecting the application sensor to the network. It has some RF module for transmitting the sensed information. It is also having the sensor parameter measurement module it is used for measuring the power level of the end device. Then the measured information also send to the coordinator depends upon the power level information the alternative paths and alternative node will alert.

Parameter Measurement:

It is used to measuring the power level of the end device depends on current and voltage parameters.

4.1. Identifying the MAC Address:

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model.A network node may have multiple NICs and each must have one unique MAC address per NIC.MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48,EUI-48 and EUI-64. The IEEE claims trademarks on the names EUI-48 and EUI-64,in which EUI is an abbreviation for Extended Unique Identifier. MAC addresses are collected from the source nodes and which is stored in the master node.

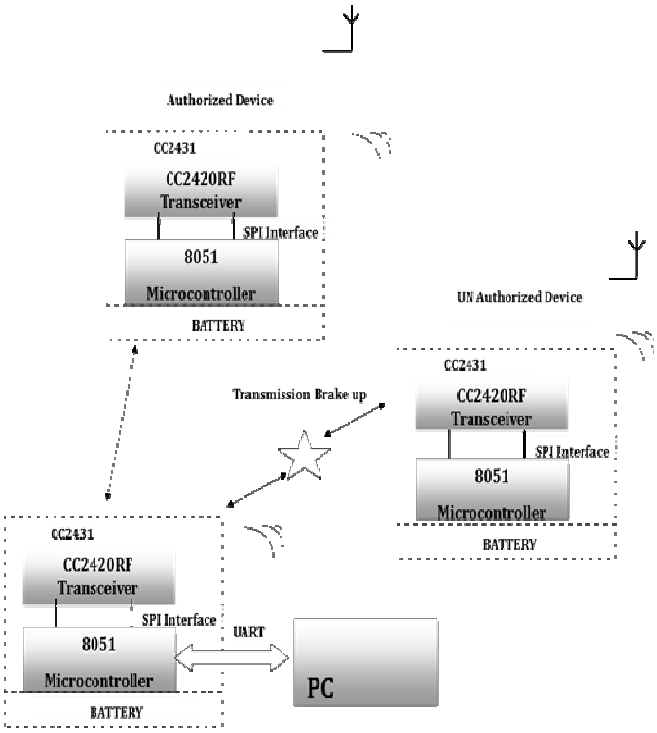

Fig.2: Hardware modules

4.2. Identifying the Failure Nodes :

In this module the hacker node is identified by the master node. The master node finds the MAC address requested by the hacker node is improper. In this module the hacker node is represented as node H. When data transmission is happening with the node D and node E the node H which finds the transmission and ready to attempt the spoofing. Once the master node identifies the hacker it gives the information to the slave nodes that the hacker is present in between the transmission path, this alerts the source nodes and to change the transmission path. This in turn moves on one the source node from current path to any other path. When the current path is changed the hacker cannot able to identify the changed path. So this enables the secure transmission.

4.3. NS-2 Simulator Basics:

NS (Version 2) is an open source network simulation tool. It is an object oriented, discrete event driven simulator written in C++ and Otcl. The primary use of NS is in network researches to simulate various types of wired/wireless local and wide area networks; to implement network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet,

Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and many more.

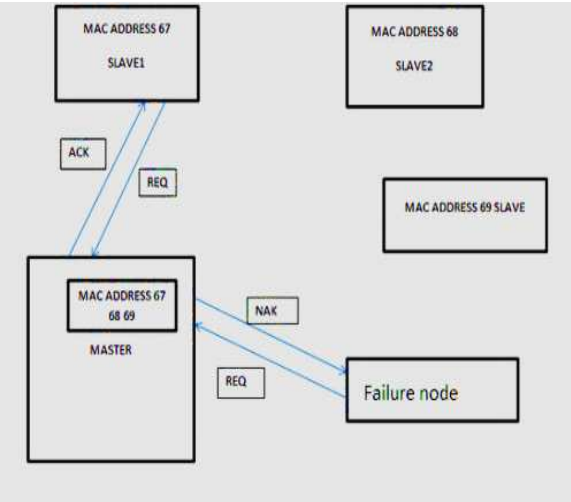

Fig.3: Identification of Failure Node

4.4. Node Creation:

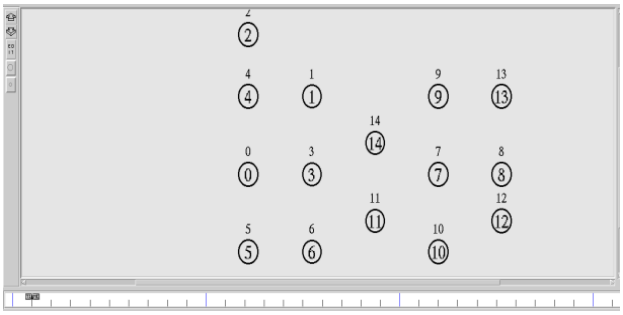

Fig. 4: Node creation

In this Fig.4 which shows the node creation , Nine nodes has been created and each node is represented as 0,1,2,3,4,5,6,7,8,9,10,11,12,13 and 14. The 0 node is the master node which controls all the other nodes. The other nodes are slave nodes which perform action whenever master node assigns the work. The nodes created by specifying the color, diameter and the axis of the circle to be placed in the block. Once the node has been created the MAC address of the nodes are to be read by the master node.

4.5.Router Updates :

The master node gathers all the necessary information about all the slave nodes. The Master node which saves the parameters of all the slave nodes, the authorization is provided only for the defined routing path.

In Fig. 5 which shows the Broadcasting information of the all the Twelve nodes. All the twelve nodes which have the specified MAC address which is unique address.

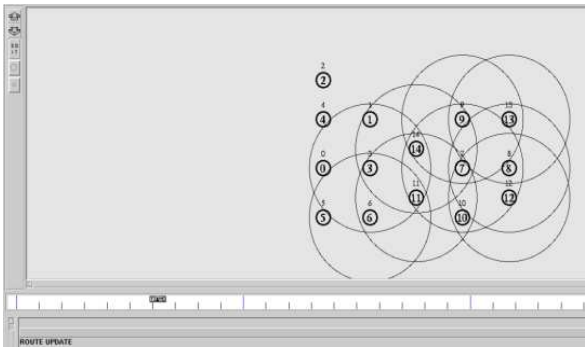

Fig. 5: Router Updates

These MAC address are identified by the master node by requesting the slave node to provide its MAC address for verification.

4.6. Detecting the Failure Node:

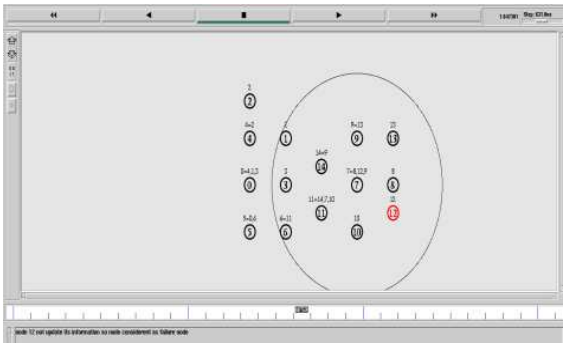

Fig.6: Detecting the Failure node

The Fig. 6 which shows the detection of the Failure node. In this system design the 12th node is represented as the failure node. The failure node which is identifies the data transmission between the node 11 and node 7. The failure node which moves closely to the data transmission path. The master node identifies the transmission path due to the openness of the wireless systems.

4.7. Data Transmission:

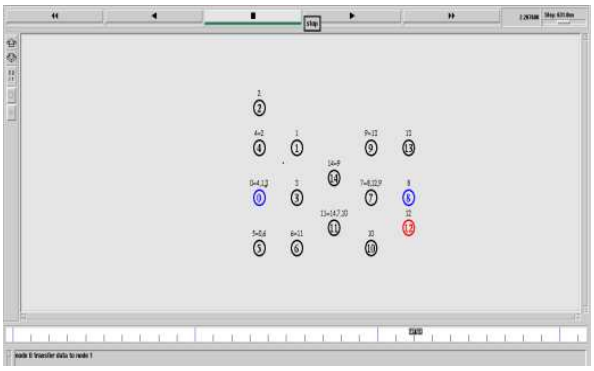

Fig. 7: Data Transmission

The fig.7 which shows the data transmission between the node 0 and node 7. Once the MAC address is master node it gives the authorization to the nodes. The node 0 having three client nodes they are 4, 1 and 5. First the date sends to node 4 then the node 4 having only one client node so data will be send to node 1 it is the dead end node so data sends to node 5. Now the node 5 is having client node 0 and 6. The node 0 is the master node so the data will be sends to node 6. The node 6 send the data to node 11 because node 6 having only one client node. The data will be send node 7 from node 11. Now the node 7 is the active node.

4.8. Data Transmission Stops:

The fig.8, which shows the data transmission, has been stopped in the node 9. When the node 9 data transmission will

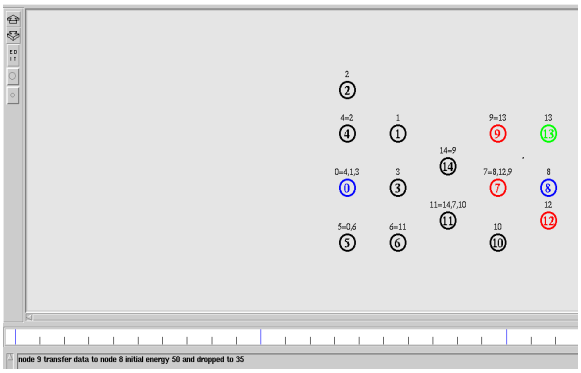

Fig.8: Data transmission stops in the node 9

be stopped at the same time the node 13 will be activated. Now the node 13 is consider as the active node. The sensed data will be transmits through node 13.

4.9. Hardware Setup :

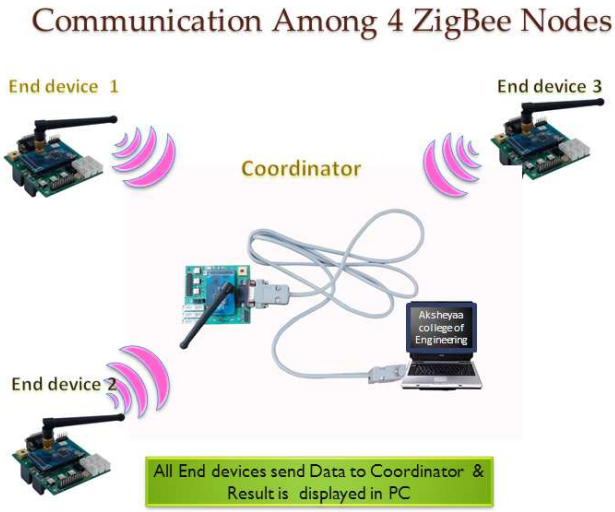

Fig.9:Hardware Setup

5. GRAPH ANALYSIS

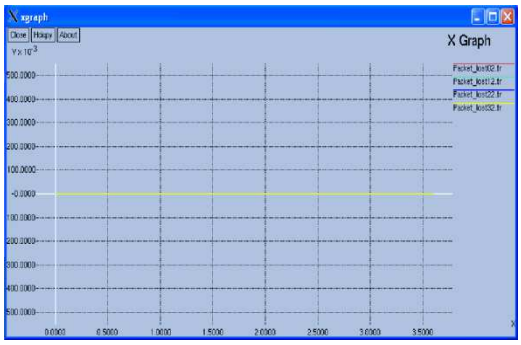

Fig.10: Packet loss analysis

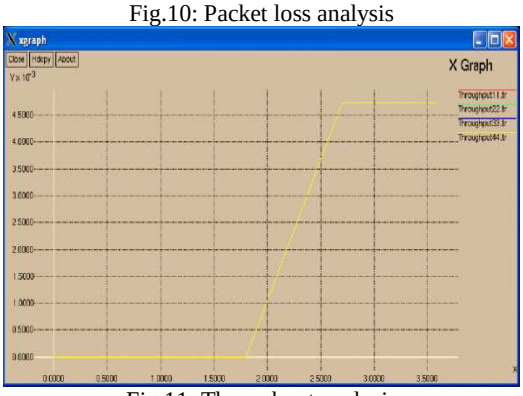

Fig.11: Throughput analysis

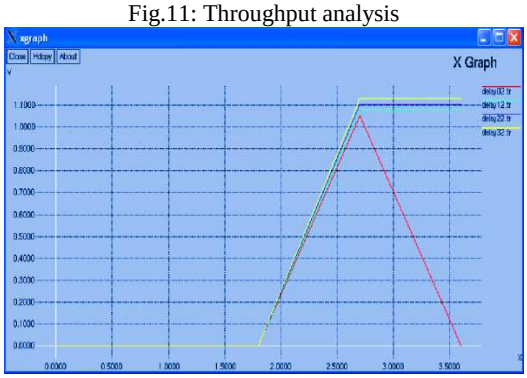

Fig.12: Packet Delay analysis

In order to obtain the effective data transmission between the nodes in the network, node failure detection and energy based routing are done successfully by PSR routing such as DSDV and BFST algorithm. Also, it makes No packet loss or data loss while the transmission. Also the overall Throughput is increase and packet delay was minimized.

6. CONCLUSION

We have proposed the system to detect and prevent the sensor node failure and energy based routing in wireless communication. The simulation of this proposed system, which we have created fourteen nodes which indicates one master node and other slave nodes. The master node identifies the failure node with improper in Broadcasting. Overall the simulation which shows how the failure node is identified and the energy based routing obtained. The advantage of this

system is to provide prevent the data loss transmission in the wireless sensor system. In the hardware section using Zigbee transceiver in each node as a future work. The Zigbee transceiver which is associated with the Zigbee protocol stack, where it contains the necessary information regarding the transceiver . In this project we are going to implement with 3 nodes to detect the failure node. The nodes can also be added in case it is needed. Thus to prevent the node failure and energy based routing in secured areas this project can be implemented.

REFERENCES

[1] C. E. Perkins and P. Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers," *Comput. Commun. Rev.*, vol. 24, pp. 234–244, Oct. 1994.

[2] Z. Wang, Y. Chen, and C. Li, "CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no.2, pp. 289–296, Feb. 2012.

[3] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," in *Proc. ACM Conf. SIGCOMM*, Philadelphia, PA, USA, Aug. 2005, pp.133–144.

[4] Rajaraman, "Topology control and routing in ad hoc networks: A survey," *ACM SIGACT News*, vol. 33, no. 2, pp. 60–73, Jun. 2002.

[5] I.Chlamtac, M. Conti, and J.-N.Liu, "Mobile ad hoc networking: Imperatives and challenges", *Ad Hoc.*, vol.1,no.1,pp.13-64, Jul. 2003.

[6] P. Larson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture, "*ACM Mobile Comput. Commun. Rev.*,vol. 5, no.4, pp.47-54, Oct. 2001.

[7] T.Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR), "*RFC 3626*, Oct. 2003.

[8] C.E. Perkins and E..M. Royer, "Ad hoc On-Demand Distance Vector (AODV) routing, "*RFC 3561*, Jul.2003.

[9] S. Murthy and J.J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks", *Mobile Netw. Appl.*, vol.1, no.2, pp.183-197, Oct. 1996.

[10] C. Hedrick. Routing Information Protocol. *RFC 1058*, June 1988.

[11] N. Santos, H. Raj, S. Saroiu, and A. Wolman, "Using ARM trust zone to build a trusted language runtime for mobile applications," in *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems*, 2014, pp. 67-80.

[12] M. Roland, J. Langer, and J. Scharinger, "Practical attack scenarios on secure element-enabled mobile devices," in *2012 4th International Workshop on Near Field Communication (NFC)* 2012, pp. 19-24.