Retrieval of Dropped and Modified Packets by Dynamic Rerouting in Wireless Sensor Networks

G. Merline
Assistant Professor, Jeppiaar Institute of Technology,
Chennai

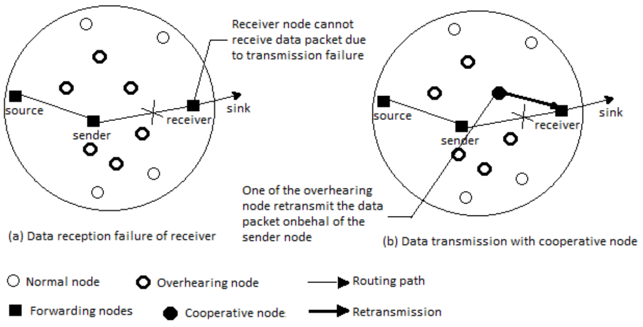
***Abstract* – In wireless sensor networks, sensor nodes are deployed in a hostile environment so it lacks physical protection and is subject to node compromise. An adversary may launch various attacks to disrupt the network communication. Among these attacks, two common attacks are packet droppers and packet modifiers, i.e., compromised nodes may drop or modify the packets that they are supposed to forward. Due to the Wireless Broadcast Advantage (WBA), all nodes inside the transmission range of a source node may receive the packet hence naturally they can serve as cooperative caching and backup nodes if the intended receiver dropped the packet. In this paper we introduced the Dynamic Rerouting with Cooperative Communication (DRCC) scheme to retransmit the dropped and modified packets. Our proposal is further validated by simulation.**

Index Terms* – *Wireless Sensor Network, Wireless Broadcast Advantage, Dynamic Rerouting with Cooperative Communication.

I. Introduction

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure and to cooperatively pass their data through the network to a main location. The modern networks are bidirectional, also enabling control of sensor activity. The development of WSN was motivated by military applications such as battlefield surveillance. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. All sensor nodes are collecting information from the environment and forwards to the base station. The base station is the main component of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN to a server.

When the source node is transmitting data packet to the sink node, the routing tree rooted at the sink is first established. When sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs the node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers/ modifiers. The dropped packets are dynamically retrieved by the proposed DRCC scheme. When the sensor nodes are transmitting a packet from source to the next hop intended node, the other nodes within the communication range of source node will overhear the packet. If the packet is dropped by the intended node then the node overheard the packet will act as a cooperative node and dynamically retransmit to the next hop node. Extensive simulation results confirm that DRCC can significantly reduce the total number of transmission and the node categorization algorithm identifies effectively the malicious nodes in the sensor network. Fig. 1 shows the system architecture of the proposed scheme,


Receiver node cannot receive data packet due to transmission failure
source
sender
receiver
sink
source
sender
receiver
sink
One of the overhearing node retransmit the data packet onbehal of the sender node
○ Normal node
○ Overhearing node
Routing path
■ Forwarding nodes
● Cooperative node
Retransmission

(a) Data reception failure of receiver

(b) Data transmission with cooperative node

Fig. 1. System Architecture

The rest of the paper is organized as follows. Section II discuss the previous work on related topics and Section III gives the models and assumptions. Section IV describes proposed DRCC in detail. Section V discusses the simulation results. Finally, Section VI concludes the paper.

II. Related Works

To identify packet droppers and modifiers a node categorization algorithm [2] is introduced. In this approach a threshold value is introduced and if the dropping ratio of the intended node is greater than the threshold value then it will be isolated from the sensor network. But the dropped packets are not retransmitted in this approach. To deal with packet droppers, a widely adopted countermeasure is multipath forwarding [5] in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated.

The watchdog method [3] was introduced to mitigate routing misbehavior in mobile ad hoc networks. It is then adopted to identify packet droppers in wireless sensor network. When the watchdog mechanism is deployed, each node monitors its neighborhood indiscriminately to collect the first-hand information on its neighbor nodes. Based on the monitoring mechanism, the intrusion detection systems are proposed in his paper. However, the watchdog method requires nodes to buffer the packets and operate in the indiscriminate mode, the storage overhead and energy consumption may not be affordable for sensor nodes. To mitigate packet droppers, introduced a widely adopted countermeasure, which is based on delivering redundant packets along multiple paths [6]. The distributed and autonomic nature of Mobile AdHoc Networks (MANET) make them prone to various forms of Denial of Service (DoS) attacks against their core functionalities, namely, routing and data forwarding. In this work, they aim to improve the end-to-end packet delivery in the presence of dropping or modification of packets by the intermediate nodes, which can prevent many misbehaviors and attacks including selfishness, black holes and gray holes. This is achieved via robust information dispersion through adaptively selected multiple node disjoint paths. The proposed solution can be considered a hybrid method for avoiding the effects of node misbehaviors through proactively dispersing information via multiple paths which are reactively tuned to avoid misbehaving nodes. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught.

By obtaining responses from intermediate nodes, alarms and detection of selective forwarding attacks can be conducted. A lightweight security scheme [10] that detects selective forwarding attacks by using a multihop acknowledgement technique that increases detection accuracy yet lowers overhead. The scheme allows both the base station and source node to collect attack alarm information from intermediate nodes. Simulation results show that the communication overhead of this scheme is usually less than 2 times the overhead of the common one-path packet delivery process, and the detection accuracy is over 95% even when the channel error rate is a harsh 15%. But this multihop acknowledgement leads to communication overhead.

A Robust Cooperative Routing protocol (RRP) is developed to retransmit the dropped packets due to the link failure in the sensor network [12]. In this scheme a robust path is established between the source node and the sink node with the equivalent nodes and remedy nodes. The equivalent node has the higher priority than the remedy node to retransmit the data packet if the ACK is not received from the sink. If there is no equivalent node overheard the data packet then the remedy node will send the reply to the source node and send the packet to the next hop.

Sensor nodes are depletes more energy when retransmitting the data packet if there is no ACK is received from the sink node. An Energy Efficient Cooperative Communication (EECC) [9] scheme is introduced to reduce the energy consumption of the sensor nodes to transmit the data packets. In this scheme the best cooperative node is selected to retransmit the packets, if the ACK is not received from the base station. A Cooperative Energy Efficient Routing Algorithm (CEERA) [8] is introduced to retransmit the packets which are dropped by the intended nodes. In this scheme, the base station will broadcast the ACK after receiving the data packet. The backoff time is calculated to the cooperative node and if the ACK is not received within the backoff time then the data packet will be retransmitted by the node which has the less backoff time.

III. MODELS AND ASSUMPTIONS

A. Network Model

We consider a sensor networks, where a large number of sensor nodes are randomly distributed in the two dimensional area and remain stationary after deployment, and all of them have similar capabilities and equal significance. All sensor nodes form a Directed Acyclic Graph and extract a routing tree from the DAG. The sink knows the DAG and the routing tree, and shares a unique key with each node. Each sensor node sends its data packets to sink nodes through multi-hop wireless links. The sink is located within the network. Assume all sensor nodes and the sink are loosely time synchronized, which is required by many applications. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighboring nodes right after deployment.

B. Security Assumptions and Attack Model

Assume that, the network sink is trustworthy and free from compromise, and the adversary cannot successfully compromise regular sensor nodes during the short topology establishment phase after the network is deployed. Compromised nodes may or may not collude with each other. A compromised node can launch the following two attacks:

Packet dropping: An adversary node drops all or some of the packets that is supposed to forward. It may also drop the data generated by itself for some malicious purpose such as framing innocent nodes.

Packet modification: An adversary node modifies all or some of the packets that is supposed to forward. It may also modify the data it generates to protect itself from being identified or to accuse other nodes.

IV. DYNAMIC REROUTING WITH COOPERATIVE COMMUNICATION SCHEME (DRCC)

Due to the broadcast nature of wireless medium, neighboring nodes of a transmitting node can overhear the packet, which is called *Wireless Broadcast Advantage (WBA).* Consider a sensor network, where two nodes sender and receiver are belong to the intended path in the sensor network. When the sender forwards the data packet to the receiver, other nodes within the communication range of sender node will also overhear the packet. The nodes which are overheard the data packet will act as a cooperative node to the sender. If there is no acknowledgement is received within the Short Inter Frame Space (SIFS) by the sender node, then the cooperative node which is closer to the receiver will retransmit the packet to the receiver.

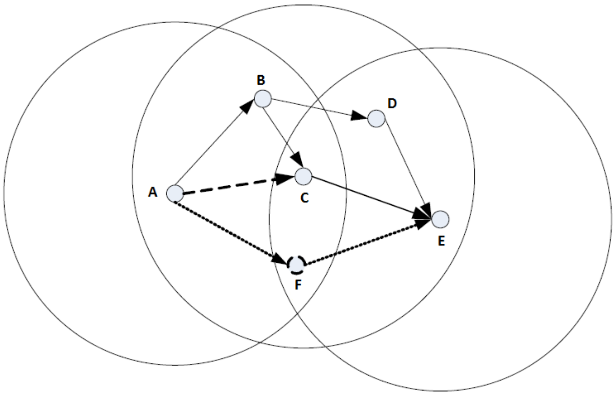


Fig. 2. Relay path with equivalent or remedy nodes.

Consider a sensor network shown in Fig. 2. where node A attempts to deliver a packet to node E over path A−C−E. When node A transmits to node C, nodes B and F may also correctly receive the packet. A guard node is at least a neighboring node of two intended nodes. In this network node B and F are the guard nodes. As guard nodes are able to take advantage of WBA, they can work cooperatively to deliver packets along the intended path. If link A−C fails due to malicious attack, then node C will drop the packet. Without waiting for potential multiple retransmissions over the same path A–C before re-routing or dropping the packet, a substitute link B−D or F−E could transfer the packet dynamically. As long as at least one link is capable of delivering the packet successfully, the packet can be received and further forwarded towards the destination. To sum up, when an intended node fails to receive a packet from its intended upstream node, guard nodes successfully receiving the packet will help forward the packet pro-actively to the downstream node(s) with dynamic rerouting.

A. *Cooperation among Equivalent Nodes*

Based on the location to the intended node, guard nodes can be classified into two categories as equivalent node and remedy node. The most preferred guard node can substitute an intended node if it is the neighbor of a pair of two-hop away intended nodes. When the replaceable intended node fails to relay the packet, the packet is blocked and goes through the guard node, then back to the intended path. Since this kind of nodes acts as the backup nodes of the intended path, this kind of nodes is called equivalent nodes. Denote Ne the set of equivalent nodes.

It is possible that several nodes will act as a equivalent nodes. To break the tie and reduce potential collisions, equivalent nodes respond to the sender after backoff time, say $T_{boe,m}$. Obviously, the node with the shortest backoff time will be the first one replying with an ACK. Once other nodes that are counting down the backoff timer hear or sense the ACK, they stop competing for relay. Thereafter, election for the relay node finishes. The backoff delay is given as,

$T_{boe,m} = SIFS + T_e P_m$, for node m $\in Ne$

Where,

$$P_m = D_m/1 - E_m$$

Te is the backoff window for equivalent nodes. *Pm* is a mixed metric of normalized link delay *Dm* and the error probability *Em* of the link between node *m* and the downstream node of the failed intended node. Link delay is the average delay experienced when forwarding a packet over the link. The backoff time for the equivalent node is no greater than *SIFS* + *Te*.

B. *Cooperation among Remedy Nodes*

If no ACK is heard or sensed before *Te* ends, it implies that no equivalent node is available. Now, the remedy nodes are allowed to compete for relaying. The remedy nodes, contains the common neighbors of an intended node and its downstream node, or neighbors of both an intended node and an equivalent node. When an intended node fails to receive a packet correctly, the packet may bypass the intended node and go through a remedy node. It travels through the remedy node, via the intended node or a guard node of the next-hop, returning to the downstream node on the intended path. Remedy nodes always have lower priority to relay than equivalent nodes. The second competition stage begins if no equivalent node transmits in the first stage. In the first stage, only equivalent nodes can be active. Remedy nodes compete with an additional backoff delay *Te* in the second stage. Denote *Nr* the set of remedy nodes and T_{bor} the backoff time for remedy nodes. Fig. 3 shows the functional architecture of the proposed scheme. The intended nodes will perform the cooperative communication by using the equivalent node and remedy node.

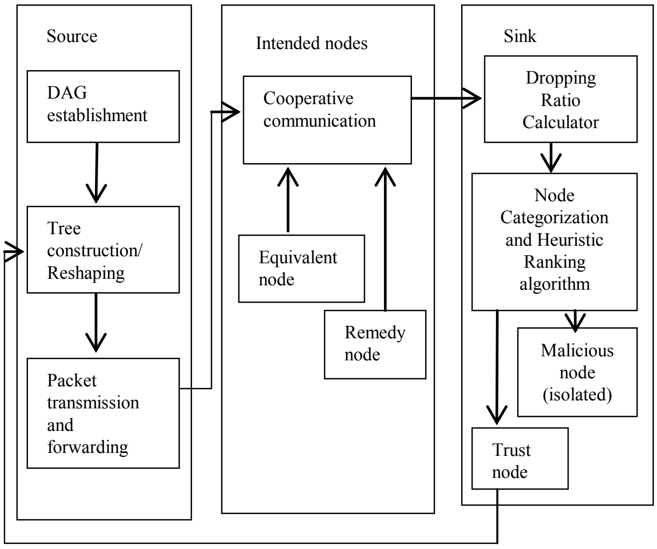

Source
DAG establishment
Tree construction/ Reshaping
Packet transmission and forwarding
Intended nodes
Cooperative communication
Equivalent node
Remedy node
Sink
Dropping Ratio Calculator
Node Categorization and Heuristic Ranking algorithm
Malicious node (isolated)
Trust node

Fig. 3. Functional Architecture

Similar to the case for equivalent nodes, they defer with backoff time,

$T_{bor,m} = SIFS + T_e + T_r P_m$, for node m $\in N_r$

Where T_r is the backoff window for remedy nodes. Any guard node hearing or sensing an ACK from another guard node assumes that a successful cooperation is completed. So it just discards the received packet.

C. *Cooperation Rules*

Based on the above analysis, we can now set the rules for coordinating cooperation among nodes. It must be noted that in DRCC only the sender nodes on the intended path can invoke dynamic rerouting for the transmitted data packet. Let *s* and *r* denote the sender and its intended receiver respectively, and *u* denotes the next hop intended receiver of *r*. E and R denotes the equivalent and remedy nodes respectively.

```
s sends a data packet to r;
while (s has not received any acknowledgement for the data packet)
  if (r receives the data packet) then
    r returns the acknowledgement to s;
  elseif (E!= Ø) then
    decrease $T_{boe}$ timer  counter  to zero;
    a packet holder E is selected as the cooperative node;
    E returns the acknowledgement to s;
    E forwards the data packet to u;
  elseif (E = Ø and R!= Ø) then
  decrease $T_{bor}$ timer  counter to zero;
    a packet holder R is selected as the cooperative node;
    R returns the acknowledgement to s;
    R forwards the data packet to r;
  elseif (E = Ø and R = Ø) then
    s retransmits the data packet to r;
  endif
endwhile
```

Fig. 4. Dynamic Rerouting with cooperative communication

D. *Node Categorization Algorithm*

In every round of packet transmission dropping ratio d_u of each node will be calculated by the sink. Based on the dropping ratio of every sensor node and the tree topology, the sink identifies the nodes that are droppers for sure and that are possibly droppers. For this purpose, a threshold Θ is first introduced. We assume that if a node's packets are not intentionally dropped by forwarding nodes, the dropping ratio of this node should be lower than Θ. Note that Θ should be greater than 0, taking into account droppings caused by incidental reasons such as collisions. The first step of the identification is to mark each node with "+" if its dropping ratio is lower than Θ, or with "_" otherwise.

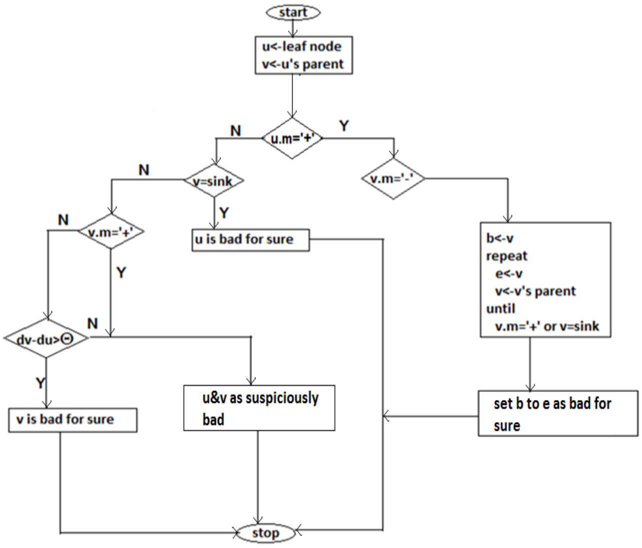


Fig. 5. A flowchart representing the Node Categorization Algorithm

In Fig. 5 the flowchart shows that the sensor nodes are categorized as bad for sure or suspiciously bad. The suspicious nodes are identified as trust node or malicious node using heuristic ranking algorithm.

E. Heuristic Ranking Algorithm

The method is based on the heuristic that, the more times a node is identified as suspiciously bad, the more likely it is a bad node. With this method, each suspicious node u is associated with an accused account which keeps track of the times that the node has been identified as suspiciously bad nodes. To find out the most likely set of suspicious nodes after n rounds of detection, all suspicious nodes are ranked based on the descending order of the values of their accused accounts. The node with the highest value is chosen as a most likely bad node and all the pairs that contain this node are isolated from sensor network. This will increase the performance of the sensor network. The process continues on the new sets until all suspicious pairs have been removed.

```
Algorithm : The Heuristic Ranking-Based Approach
sort all suspicious nodes into Q according to the
descending order of their accused account values
S'<-null
for each pair in S do
   {
    if S!=null
       u<-deque(Q)
    S'<-S'^{u}
   }
remove all {u} from S .
```

Fig. 6. Heuristic Ranking Algorithm

V. Performance Evaluation

\

The proposed DRCC scheme has been implemented and analysed in the network simulator NS2. The proposed scheme retrieves the dropped and modified packets effectively with reduced number of retransmissions. We evaluate the performance of DRCC in terms of packet delivery ratio and average end to end delay and comparison of trusted nodes and malicious node with various simulation time.

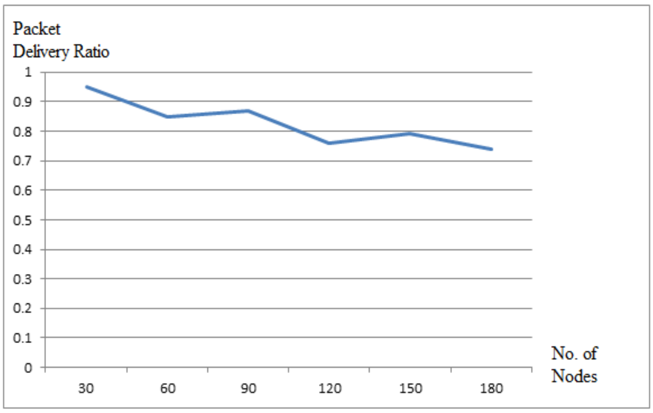


Fig. 7. Performance with Trusted Nodes

Packet transmission will be performed for various simulation times and the dropping ratio will be calculated for each transmission. Now using node categorization algorithm and heuristic ranking algorithm the malicious node will be identified and isolated from the sensor network. Based on the simulation time and the dropping ratio the graph will be designed. Fig. 3 shows the performance of sensor network with different number of sensor nodes. Packet delivery ratio is calculated for each packet transmission by varying the number of nodes in the sensor networks. When the number of nodes is increased the packet dropping by the nodes also increased and therefore the delivery ratio will be decreased. Fig. 7 shows the graph representation for packet delivery ratio with varied number of nodes.

The dropping ratio of the trusted node with cooperative communication and the malicious node is calculated for number of rounds with different simulation time and the graph is designed based on these values. Based on the values the graph will be designed and it is shown in the Fig. 8. The trust node has the minimum dropping ratio values whereas the malicious node has the greater values.

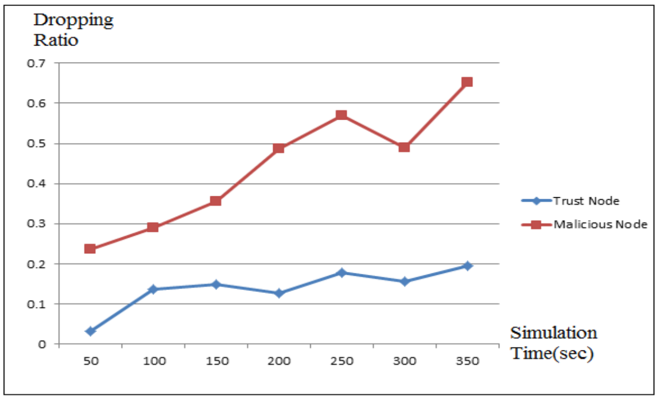


Fig. 8. Comparisons of Packet Loss in a Network with Trusted Nodes and Malicious Nodes

VI. Conclusion

In this paper, we proposed a dynamic rerouting with cooperative communication scheme (DRCC) for unreliable sensor networks. This new scheme takes advantage of cooperative transmission to enhance the dynamic rerouting against malicious nodes. A best co-operator is elected from qualified neighbours of the relay node on the routing path to participate in the data transmission. In this way the DRCC scheme can retrieve the dropped and modified packets in sensor network. Node categorization algorithm is used to identify and isolate the malicious nodes which are dropping the packets in the sensor network. Through analysis and experiments, we validate that DRCC is capable to retrieve the dropped and modified packets in wireless sensor networks.

References

1. Bin Li, Wenjie Wang, Qinye Yin, Duo Zhang, Rong Yang, Li Sun "Energy-efficient Cooperative Geographic Routing in Wireless Sensor Networks Utilizing Transmit Diversity and Multi-sensor Diversity," Vehicular Technology Conference (VTC Fall), pp. 1-5, 2011.
2. Chuang Wang, Taiming Feng, Jinsook Kim and Guiling Wang "Catching Packet Droppers and Modifiers in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, No. 5, pp. 835- 843, May 2012.
3. Giuli T., Marti M. and Baker M. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom , 2000.
4. Jan Nikodem, Ryszard Klempous, Maciej Nikodem and Zenon Chaczko "Neighbors Cooperation in WSN Based on Collective Decisions," IEEE 16th International Conference on Intelligent Engineering Systems, pp. 139- 143, June 2012.
5. Luo H., Ye F., Lu S. and Zhang L. "Statistical En- Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, vol. 23, pp. 839-850, 2004.
6. Miremadi S.G., Kefayati M., Rabiee H.R. and Khonsari A. "Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. Fourth ACM Workshop Security of Ad Hoc and Sensor Networks, 2006.

7. Rosberg Z., Liu R. P., Dong A. Y., Tuan L. D. and Jha S. "ARQ with Implicit and Explicit ACKs in Wireless Sensor Networks," IEEE "GLOBECOM" 2008.
8. Sami S. Alwakeel and Najla A. Al-Nabhan "A Cooperative Learning Schheme for Energy Efficient Routing in Wireless Sensor Networks," 2012 11th International Conference on Machine Learning and Applications, pp. 463-468, 2012.
9. Weiwei Feng, Feng Liu, Fengnan Yang, Lei Shu and Shojiro Nishio "Energy-Efficient Cooperative Communication for Data Transmission in Wireless Sensor Networks," IEEE Consumer Electronics Society_, vol. 56, pp. 2185-2192, 2010.
10. Xiao B. and Yu B. "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," Proc. 20th Int'l Symp. Parallel and Distributed Processing, 2006.
11. Xiao B., Yu B. and Gao C. "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," J. Parallel and Distributed Computing, vol. 67, pp. 1218- 1230, 2007.
12. Xiaoxia Huang, Zhai, Yuguang Fang "Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 7, no. 12, pp.5278-5285, Dec 2008.
13. Ye F., Yang H. and Liu Z. "Catching Moles in Sensor Networks,"Proceeding of 27th International Conference on Distributed Computing Systems, pp. 69-78, 2007.
14. Zhang X., Jain A. and Perrig A. "Packet-Dropping Adversary Identification for Data Plane Security," Proc. ACM CONEXT Conference, 2008.

G.Merline has completed her B.E, Electronics and Communication Engineering in Jeppiaar Engineering College, Chennai and M.E, Communication Systems in Easwari Engineering College, Chennai. Her areas of interest include Network Security and Image Processing. She is currently working as an Assistant Professor in Jeppiaar Institute of Technology, Chennai.