*International Journal of Latest Engineering and Management Research (IJLEMR)*
*ISSN: 2455-4847*
*www.ijlemr.com || Volume 03 - Issue 02 || February 2018 || PP. 66-73*

# A Proactive Routing Protocol to Secure Wireless Sensor Networks

N. Vidhya,
*Research Scholar, Bharathiar University, Coimbatore, India*

Dr. P. Sengottuvelan,
*Associate Professor, PG Extension Centre, Periyar Univeristy, Dharmapuri*

**Abstract:** The WSN network are prone to malicious attack, as any device that falls within the frequency spectrum can penetrate the network. Also as the network keeps changing, a dynamic secure routing is much needed. In this paper the focus is in providing a secure Wireless Sensor Network by staggering frequency at which the data is transmitted. This paper discusses preventing any possibility of resource exhaustion attack, by altering frequency of packet transmission from time to time over the Optimized Link State Routing Protocol (OLSR) and Destination Sequence Distance Vector Routing Protocol (DSDV) is attempted. It also discusses the recent advancement in wireless sensor network along with the architecture required for a dynamic secured routing. Sensor nodes in the network move in various patterns providing mobility configurations influencing the network. This concept provides high security in the confidential fields thus helps in areas of application such as Military provinces.

**Keywords**: Wireless Sensor Network, energy, routing, attacks, DSDV, OLSR.

## 1. Introduction

WSN itself is a challenging topic that plays a vital role in day to day life. The change in the topology is the main factor which affects the network lifetime of the WSN applications. In WSN architecture having stationary nods, the change in the topology occurs due to any node failure. The node failure generally occurs because of the energy depletion or congestion in the network. However, in the mobile Wireless Senor Network, the main reason of the topology change is caused by the node movement which is called the dynamic WSN. Sensor nodes in the network may move in any patterns, and varying mobility configurations have profound influences on the network.

Nowadays, WSN are used in critical fields such as military, places of natural calamities. Sensor networks are realized on the battle field by deploying cheap, throw-away sensors. Hence a battle field operation does not suffer the consequence of any kind of antagonistic action unleashed on the wireless sensor networks. This specific characteristic makes it more suitable for battle field operations. As such military makes use of this technology to its advantage for wide range of purposes starting from monitoring of forces to detecting biological or chemical detection. However, deployment of WSN for motion detection from the security perspective is time tested. Cryptography is the prime existing security enforcement approach that demands heavy computing resources. And WSNs are highly resource scanty. In order to prevent any possibility of resource exhaustion attack, an improvement of altering frequency of packet transmission from time to time over the Optimized Link State Routing Protocol (OLSR) and Destination Sequence Distance Vector Routing Protocol (DSDV) is attempted.

### 1.1 Issues in WSN

Node outage is a phenomenon that brings down the WSN's components, that could be a cluster-leader or a sensor node or any other devices that form the WSN. The effective causes could be causing physical or logical damage to the network components. At the Link layer seizing up of data packets thus effectively preventing data movement from source to destination, and depleting network resources leading to chaos.

Collision attacks are kind of attack that are realized by altering the header contents of message packet possibly in both direction. This may cause corruption and cripple the network by dropping the packets transmitted. It can also cost energy exhaustion.

Resource exhaustion attack can be exemplified by an example which has a malicious node with node number 25 among a network of 26 nodes. The node 25 generates repeated collisions resulting in a stream of retransmissions and of out-of-date, dead and corrupted packets and eventually resulting in crippling the sensor node, the condition otherwise known as node death. The malicious node has to establish the path between itself

and the target node. This is done by a broadcast of Route Request message (RREQ) that helps in finding the path to the target node.

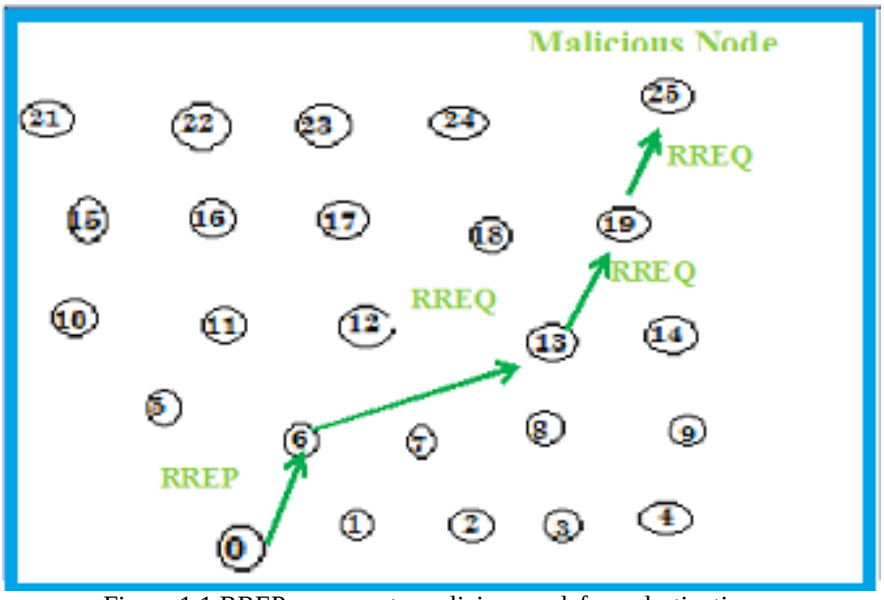


Figure 1.1 RREP message to malicious nodefrom destination

### 1.2 Resource Exhaustion Attack

Among the different types of attacks that have been discussed, the 'Resource Exhaustion' attack is the focused area. As discussed earlier the existing techniques makes use of standard cryptographic algorithms which demand heavy computing resources, namely memory, processing power and energy, which are essentially scarce in the wireless sensor networks.

Wood and Stankovic define one of the kinds of denial of service attack as "any event that reduces or get rid of a network's capacity to perform its expected function". The DoS attack is not new, still it is able to attract the research communities. In addressing this security issue, the localized encryption and authentication protocol (LEAP) uses 4 different types of keys which again unfortunately bring the problem of resource exhaustion due to implementing mechanisms of the key management.

### 1.3 Proactive Routing Protocol for Resource Exhaustion Attack

The two important categories of routing protocol in WSN are proactive and reactive. Proactive protocols used to maintain updated lists of destinations and the corresponding routes. The routing information is updated by periodically exchanging routing tables across the entire network elements, whereas, the reactive protocols find a route only when needed (on demand) by broadcasting the RREQ packets (Zhao & Ammar 2003, Rahman et al 2010). The advanced proactive protocols have been chosen for this research for the limited resources of WSN's. This research adopts Optimized Link State Routing Protocol (OLSR) and Destination sequence Distance Vector Routing Protocol (DSDV) which maintains routing information (Pandey & Baliyan 2012, Rahman & Zukarnain 2009). The OLSR is used for the mobile ad hoc networks as well as for wireless ad hoc network.The link state information is periodically discovered and propagated across the MANET using user hello message and topology control messages by the OLSR. The identification of next hop by individual nodes is computed by shortest hop forwarding paths (Jose Carlos et al 2011).

The proactive characteristic of the protocol provides that the protocol has all the routing information to all participated hosts in the network (Ge Kunz & Lamont 2003). The DSDV protocol is a table driven protocol. This routing protocol solves the routing loop problem (Tuteja et al 2010). The entries in the routing tables is associated with a sequence number which usually in a even number in case the link is available, it is odd otherwise. This sequence number is generated by the destination. The routing information is shared among the nodes in two quanta. One is as a full dump at lesser frequency than the incremental updates at higher frequency. The availability of paths across all nodes in network favors proactive algorithm being chosen as the delay in path establishment. Also the latency for the route discover seems to be low and a loop free path is promised. Hence proactive routing protocol is well suited for the limited resource of WSN. Here multiple paths are taken depending on the size of the data that has been transmitted. Depending on the threshold limit, the protocols vary.

The proactive routing protocols stores the paths to destinations in the routing table periodically, if in case of any attacks the paths could be shuffled.Also the latency for the route discover seems to be low and a

loop free path is promised. Hence proactive routing protocol is well suited for the limited resource of WSN. Here multiple paths are taken depending on the size of the data that has been transmitted. Depending on the threshold limit, the protocols vary. The proactive routing protocols stores the paths to destinations in the routing table periodically, if in case of any attacks the paths could be shuffled.

### 1.4 Qualitative and Quantitative Metrics for Protocol Evaluation

**Qualitative metrics include:**

i) **Security**: The routing protocols must implement supporting mechanism for security. This is found essential as each node that participates in routing is a vulnerable entity in ant MANET (XiuliRen & Haibin 2006).
ii) **Loop freedom:** MANETs have limited resources. The nodes while computing the paths must avoid loop formation in the network. Thus the network must be free from loops so as to get rid of wasteful resource consumption of energy in terms of processing time, power, and bandwidth. The nodes might be using any of the popular algorithms like Bellman–Ford algorithm for computing the path information.
iii) **Sleep mode:** MANETs are usually powered by batteries. Sleep mode is the condition in which the node effectively goes off for a short duration with an objective of conserving power. Often it is aimed at no degradation in the performance of routing or any other algorithms.
iv) **Unidirectional link support**: It is always desirable of any routing protocol to be able to support that the nodes links for both one way or two way communication.
v) **Multicasting**: Nodes shall support multicast communication in real-time across the network.
vi) **On-demand routing behaviour:** On - demand or reactive routing has an advantage of minimal control packet dissemination which considerably reduces the bandwidth consumption and improves the available bandwidth for user applications but at the cost of relatively higher latencies. It is always a good idea to maintain a balance. Minimum latency and maximum delivery ratio are of paramount importance in the case of high speed networks even with a marginal increase in routing overheads. The case is quite opposite in the case of radio network device wherein energy consumption is given importance.

**Quantitative metrics include:**

i) **Route acquisition time:** It is the time taken to discover a route from source to destination. The route acquisition time and network latency are directly related.
ii) **Out-of-order delivery:** It is a measure expressed in percentage of number of packets delivered out-of-order over total number of packets delivered. The higher-layer protocols would be more efficient when packets are received in the same order in which they had been sent.
iii) **Efficiency:** This can be looked up on from two perspective i.e. one from bandwidth utilisation in route discovery and another from packet delivery ratio.
iv) **Packet Delivery Ratio:** This is the ratio of number of packets sent from the source to the number of packets received at the destination.
v) **Average end-to-end delay:** This is the average time delay for data packets from the source node to the destination node.
vi) **Normalized routing load:** It is defined as the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes.

### 1.5 Changing and Verification of the Frequency

In order to avoid resource exhaustion attacks that is attacks on the resources that are available. The application of different frequencies has been proposed. The different frequencies that are allotted use the technique that the Radio Frequency Identification (RFID) uses. The mechanism of RFID is used in the proactive protocols such as the OLSR and DSDV. This is done in order to have secure data transmission also to avoid resource exhaustion attacks.

Consider 40 channels with different frequencies that are taken into consideration. If any intruder tries to attack, leaving the attacked channel, we will have 39 channels. It is desirable to keep the probability of intruder gaining access to the channel small. This can be achieved by increasing the number of frequencies used in the network or / and by introducing the frequency variation time to a random interval. The two earlier protocols namely OLSR and DSDV support a variety of headers viz. Trace header, RTP header, TCP / UDP header, IP header and common header. A common header serves the purpose of adding custom fields.

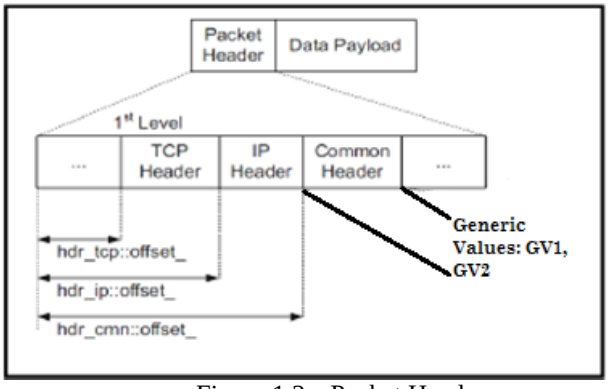


Figure 1.2 Packet Header

In order to implement this, adding two fields in the common header part of the packet header is suggested. These fields store two generic values GV1 and GV2 that are generated before the packet transmission. These generic values allow the receiver to know the malicious packet frequency for the purpose of rejecting them. In this way the receiver will not waste the resources in treating the malicious node that is the node 25.

```
Double GV1;
Double GV1;
// Creating two random variables to store the generic number
GV1= Generic number;
GV2 = Generic number;
// Setting two generic values. The generic values are between 0 and 1:
if (GV1 <= GV2)
{ Send packets using frequency number 1; }
else
{ Send packets using frequency number 2; }
// Setting the frequency according to message length (l) and of packets received (r):
If (GV1 + GV2 <= 2) && (GV1 + GV2 >= 0)
{
// Verification of the generic values:
If (GV1 <=GV2 ) { Generic Frequency =1;}
else { Generic _Frequency =2;}
}
Else { Drop (packet); }
// Setting the frequency according to message length (l) and of packets received (r):
If ( Random Frequency != Incoming packet frequency )
{ Drop (packet); }
// Checking if the Generic Frequency will be the same as the incoming packet frequency:
Else
// Continue with either of the advanced proactive protocol.
```

Figure 1.3 Changing and verification of the frequency

The Figure 1.5 shows the changing frequency before the packet transmission and also the frequency verification at the packet reception is shown. Before transmitting the packet through the advanced proactive routing that through advanced DSDV (ADSDV) and advanced OLSR (AOLSR) for a secure transmission, the frequency is set to either 1 or 2. The generic variables GV1 and GV2 whose data type is double and will keep the generic number generated in order to use them at the receiving end. When the packet is received at the end, the advanced proactive protocol either advanced OLSR or the advanced DSDV will check the generic value and

the incoming frequency. If the packet frequency is not same at the transmission side and the receiving side according to the generic number that has been attached to the packet, then the packet is discarded. If the frequency is the same to the frequency generated by the generic numbers, the packet will be accepted.

### 1.6 Results Obtained Through Simulation

The Network simulator has been used for the obtaining the results. The Figure 5.6 shows the simplified view of the network simulator 2(NS2). NS-2 takes as an input a TCL file (in which the implemented scenario is present). C++ and Object-oriented Tool Command Language (OTcl) are the two key languages that are being considered by NS2.

Table 1.1 Network Parameter

| Parameter | Value | Description |
|---|---|---|
| **Val (Chan)** | Channel/ wireless channel | Channel Type |
| **Val (mac)** | Mac/802_15_4 | IEEE standard |
| **Val (nn)** | 26 | Number of nodes |
| **Val (rp)** | Advanced OLSR (AOLSR), Advanced DSDV (ADSDV), Advanced Proactive Routing protocol (APRP) | Routing protocol |
| **Val (x)** | 50 | Setup topography object |
| **Val (y)** | 50 | Setup topography object |
| **Val (stop)** | 50 | Simulation time |

Table 1.1 shows the network parameter that has been used in a TCP file in NS2 simulation. The first parameter expresses to the simulator that the channel by which the node transmits and receives packets. It can be wired or through wireless channels. The IEEE 802.15.4 standard has been used in the simulation that defines the physical layer and the media access control. Val (nn) defines the total number of nodes taken into consideration, which is set to 26 that is from node 0 to node 25. Val (rp) is set to the advanced proactive protocol that consists of Advanced OLSR (AOLSR) and Advanced DSDV (ADSDV), which signifies the routing protocol used in the ns2 simulation. Val (x) and val (y) are the topography object that are set equal to 50 meters. So 50 m² is the simulation area that has been set for the proposed scenario. Val (stop) represents the simulation time at which we need to stop the simulation, and is set to 50 second.

The Figure 1.4 shows the throughput analysis of the dropping packets that comes out of the malicious node that is the node 25 which is present at the receiving node. Figure 1.5 shows the energy that has been used by the AOLSR and ADSDV; the target node will not waste its energy.

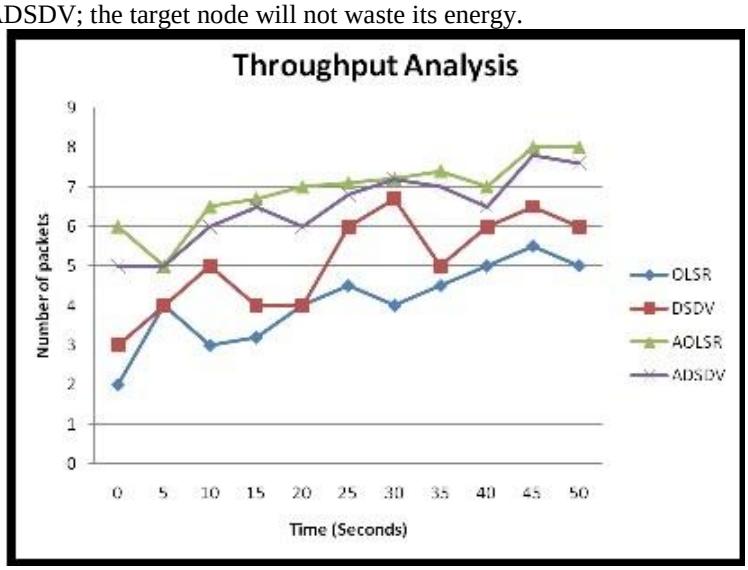


Figure 1.4 Throughput of the dropping packets at the destination node

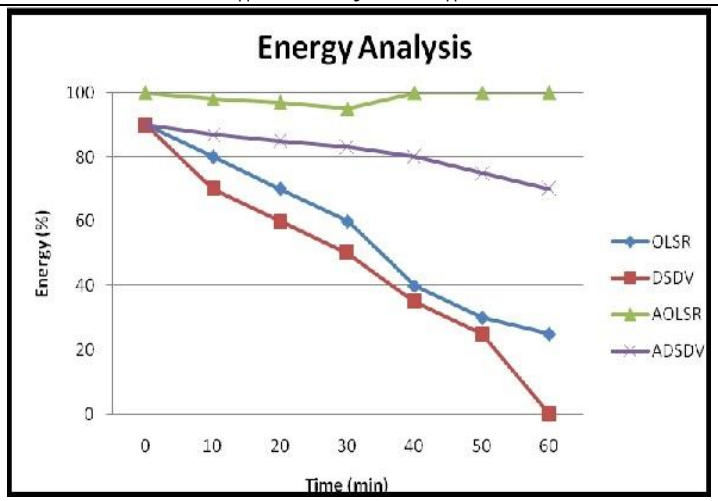


Figure 1.5 Energy level over time of the victim node

Latency is the time interval between the simulation time and the time taken to respond. The latency is said to have half of the round trip time. Few samples are taken for calculating the time taken for a packet to travel from source node to the sink node. The latency analysis is shown in Figure 1.6. The latency of the ADSDV seems less when compared to the other three techniques. The maximum latency obtained is 450ms by DSDV and the minimum latency obtained is 90ms AOLSR.

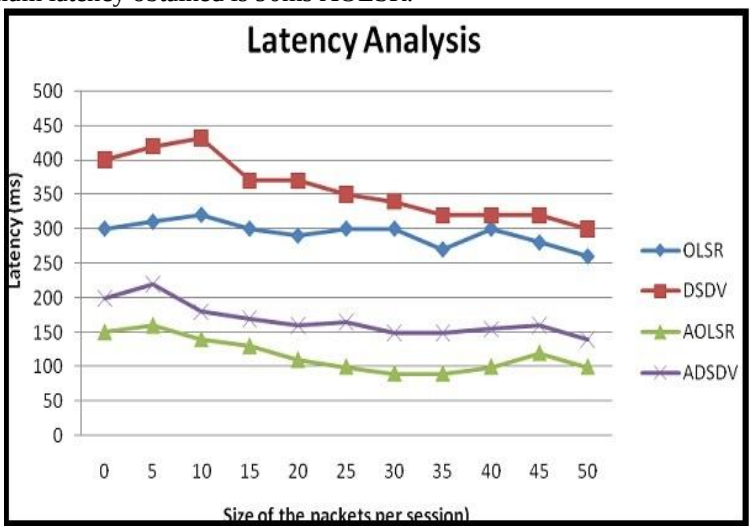


Figure 1.6 Latency Analysis

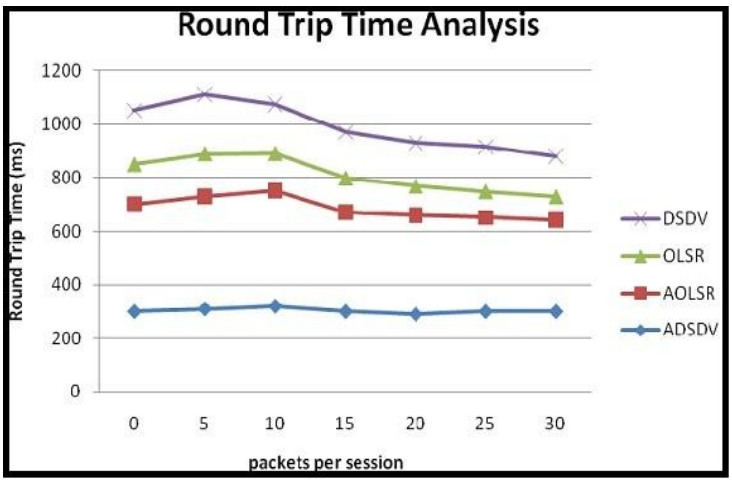


Figure 1.7 Round Trip Time Analysis

The round trip time is the total time required for a packet to travel from the source to the destination and also from destination to source. ICMP is used in sending and receiving the packet between the nodes that are involved in the transmission. The round trip time analysis is given in Figure 1.7. The DSDV takes the maximum round trip time whereas the ADSDV take minimum round trip time.

The success rate is the number of packets delivered safely at minimum time consumed. The nodes that followed advanced OLSR delivered almost all the packets that were sent. The nodes that followed DSDV delivered less number of packets than compared to other methods. Success rate analysis is shown in figure 1.8.

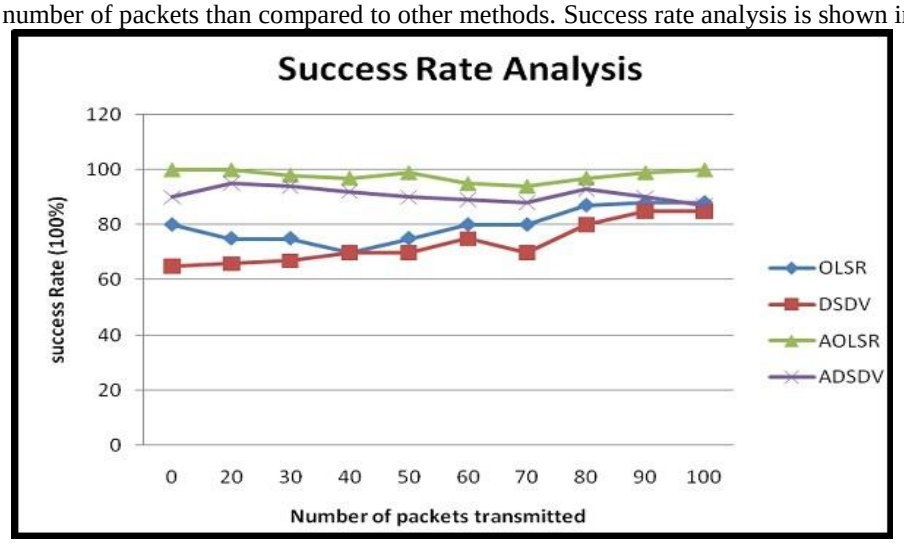


Figure 1.8 Success Rate Analysis

## 1.7 Conclusion

In this paper an approach based on changing the frequency in the Advanced OLSR and advanced DSDV protocol, which is a proactive routing protocol, has been proposed implemented and verified. The main goal was to avoid resource exhaustion attack. The resource exhaustion attack has been shown using a scenario. The scenario has been simulated using NS-2. The simulation results showed that a target node will not waste its resources treating the malicious packets. Changing the frequency of packets transmission in order to secure a WSN from the resource exhaustion attack, may be useful for many fields, such as in the military application.

## 1.8 References

[1]. V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-tolerant networking architecture," Network Working Group RFC 4838, Apr. 2007.

[2]. K. Fall, "A delay-tolerant network architecture for challenged internets," in Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ser. SIGCOMM '03, Aug. 2003, pp. 27–34.

[3]. Q. Fu, L. Zhang, W. Feng, and Y. Zheng, "Dawn: A density adaptive routing algorithm for vehicular delay tolerant sensor networks," in Annual Allerton Conference on Communication, Control, and Computing (Allerton), Sept. 2011, pp. 1250–1257.

[4]. K. Scott, T. Refaei, N. Trivedi, J. Trinh, and J. Macker, "Robust communications for disconnected, intermittent, low bandwidth (dil) environments," in Military Communications Conference (MILCOM), Nov. 2011, pp. 1009–1014.

[5]. Y. Zhuang, J. Pan, Y. Luo, and L. Cai, "Time and location critical emergency message dissemination for vehicular ad-hoc networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 1, pp. 187–196, Jan. 2011.

[6]. T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in Proceedings of the ACM SIGCOMM workshop on Delay-tolerant networking (WDTN), Aug. 2005,pp. 252–259.

[7]. Z. Feng and K.-W. Chin, "A unified study of epidemic routing protocols and their enhancements," in IEEE International Parallel and Distributed Processing Symposium Workshops &PhD Forum (IPDPSW), May 2012, pp. 1484–1493.

[8]. A. Lindgren, A. Dpria, E. Davies, and S. Grasic, "Probabilistic routing protocol for intermittently connected networks," Internet Research Task Force (IRTF) RFC 6693, pp. 1–112, Aug. 2012.

[9]. A. Balasubramanian, B. N. Levine, and A. Venkataramani, "Replication routing in dtns: A resource allocation approach," IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp.596–609, April 2010.

[10]. X. Ma, "Coupling degree seeking based routing strategy for delay tolerant networks," in International Conference on Signal Processing Systems (ICSPS), vol. 1.

[11]. P. P. Joby, P. Sengottuvelan, " A Localised clustering scheme to detect attacks in wireless sensor networks" International journal of electronic security and digital forensics, vol 7, No.3,2015.

[12]. X. Wang, Y. Shu, Z. Jin, and H. Chen, "Directional forward routing for disruption tolerant networks," in Asia-Pacific Conference on Communications (APCC), Oct. 2009, pp. 355–358.

[13]. A. Bujari, C. Palazzi, D. Maggiorini, C. Quadri, and G. Rossi, "A solution for mobile dtn in a real urban scenario," in IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Apr. 2012, pp. 344–349.

[14]. H. Mei, P. Jiang, and J. Bigham, "Augmenting coverage in a cellular network with dtn routing," in IEEE Wireless Communications and Networking Conference (WCNC),Mar.2011,pp.516–521.

[15]. M. Haibo, J. Peng, and J. Bigham, "Augment delay tolerant networking routing to extend wireless network coverage," in International Conference on Wireless Communications and Signal Processing (WCSP),Nov.2011,pp.1–5.

[16]. S.-H. Kim and S. Jae Han, "Contour routing for peer-to-peer dtn delivery in cellular networks," in International Conference on Communication Systems and Networks (COMSNETS),Jan. 2012,pp.1–9.

[17]. W. Jianjian and W. Ronghui, "A routing algorithm based on energy constraint," in International Conference on Computer Research and Development (ICCRD), vol. 2, Mar. 2011, pp.330–332.

[18]. P. P. Joby, P. Sengottuvelan, "On the Construction of Virtual Topology Structure for Secure Routing in Wireless Sensor Networks" Sensor Letters, vol 13, no 11, pp 946-952, 2015.