DETECTING BLACK HOLE ATTACK USING FUZZY TRUST APPROACH IN MANET

[1]S.Abinaya [2]G.Arulkumaran

[1]PG Student Information Technology, Vivekanandha College of Engineering For Women(Autonomous),Namakkal,India

[2]Assistant Professor Information Technology, Vivekanandha College of Engineering For Women (Autonomous), Namakkal, India

[1]sekar.abinaa5@gmail.com, [2]erarulkumaran@gmail.com

Abstract: Wireless communication is vital during disasters, natural climates and military operation. Military application required secure way of data transmission and protect data from third party. However in MANET due to dynamic topology the nodes are prone to various security attacks like modifying the data, sniffing the information, inhibited by limited energy, computational power and bandwidth. Black hole is one of the possible attacks in MANET. We propose fuzzy logic scheme to detect black hole attack based on certificate authority and trust node to improve the performance of AODV. Fuzzy is a mathematical logic that attempts to solve problems by assigning values to an imprecise spectrum of data. Fuzzy logic detect misbehaving node by giving certificate to only trusted node. The proposed technique is more secure and reliable in military data communication.

Keywords: MANET, AODV, Fuzzy logic, Security in Military Application.

1. INTRODUCTION

A mobile ad-hoc network (MANET) is infrastructure less and self configuring network. MANET is particularly vulnerable to security attack because of its uniqueness. Each device in MANET is free to move autonomously in any direction and will therefore change its links to other devices frequently. MANET is a type of ad-hoc network that can change location and organize itself on the fly. Because MANETs are mobile devices, they are wireless link to connect to various networks. MANETs are easy to set up and use since their operation does not depend on any fixed communications. There are many applications that can benefit from MANETs such as:

- Military tactical operations: A communication network that relies on a certain infrastructure is not desirable for military deliberate operations, as it constitutes a soft spot in hostile environments. Elimination of the need for the hard/impossible to set up fixed infrastructure makes MANETs perfect candidates for such operations.
- Search and rescue missions: Oftentimes search and rescue missions are performed in remote locations with no communication communications, such as the top of a mountain, the middle of a forest or inside a cave. MANETs are easy to use communication systems for such scenarios.
- Disaster relief: MANETs provide communication in environments where existing communications is destroyed or left inoperable.
- Law enforcement: Law enforcement operations can be extended to include locations with no communication infrastructure. MANET systems provide fast and secure communication in such scenarios.
- Commercial use: MANETs can be used to support data swap over between people and applications in large meetings and conventions.

MANETs are unique among communication networks, as can be experiential from the vital application areas. However, the unique characteristics required by these applications necessitate unique

solutions and differentiate MANETs from other conservative networks. There are various challenges that have to be taken into account when designing a MANET.

First of all, the communication channel between the nodes in the network is highly unreliable. A MANET operates over wireless channels that incur higher bit errors compared to wired interfaces. MANET protocols have to be designed with the assumption of an erroneous channel. MANETs also are designed to work in any environment, whether it is a desert, forest or hilly region. The lack of a- prior knowledge about the propagation characteristics of the wireless medium also presents challenges to protocol design for MANETs. Node mobility is another challenge in the design of MANETs. The topology of a MANET can change not only with changing propagation characteristics of the medium but also due to the mobility of the nodes in the network. In order to reliably convey information, MANET protocols have to include mechanisms for proper mobility organization. Having limited storage and computational capabilities further restrict the range of algorithms that can be used in MANETs.

In MANET the energy of one node is powered by batteries with limited energy. Therefore the minimal energy node can roll as selfish node. The energy of a node is calculated by the energy spent on broadcast and the reception of data packets and acknowledgments. MANET attracted by the attackers because its unique features like lively topology, variable capacity, open medium, local physical security and energy constrained operation. The attackers can easily eavesdrop the message because there is no physical connection, because of user mobility or node failure MANET faces technical challenges due to severe resource restraint like vulnerability, unreliable communication and memory size. In military application mobility is a critical factor because mission will start at sure coordinate and will end up at the other coordinate. In the battle field soldiers swap the message like voice recording, video tapes, images and quality of services to other field unit. Unfortunately the communication can have delay of message, dropped message and delivery of erroneous. To improve the performance the proposed scheme provides trust based data exchange, certificate authority and fuzzy based analyzer to detect the misbehaving node.

Adhoc on Demand Distance Vector routing algorithm used in military request because the source node maintain the routes as long as need by itself. When source node need new shortest path to purpose, based on route request (RREQ) and route reply (RREP) it can create new path. This route is updated automatically in routing table for all destinations to find better route. In a black hole attack, the malicious node advertises itself that it has valid route to destination. This malicious node is first to reply for the RREQ message and drop all the packets between source and destination resulting in denial of service.

Moreover, MANETs have limited bandwidth and energy resources. The supposition of mobility inherently limits the energy supply available at each node. Thus, it is important for a MANET to be power efficient and energy aware. Typically, the bandwidth available for the communication is also incomplete. The erroneous channel characteristics further decrease the channel capacity, making bandwidth a valuable resource for MANETs. Efficiency in using the bandwidth and energy capital and a carefully adjusted spatial reuse algorithm are some of the key criteria for the design of MANET algorithms.

Black hole attack is one of the widely used attacks against routing protocols. In this attack, malicious nodes insert fault routing information to the source node and lead all data packets towards themselves, then drop all them. Based on the number of malicious nodes, black hole is divided as single black hole attack. In single black hole there is just one malicious node is obtainable in the network while in cooperative black hole, there are more than one malicious node is presented in the network.

Detecting the cooperative malicious node is highly challengeable, since malicious node uses some methods to cover their tracks and make it harder for other nodes to detect them. False position is another key challenge in helpful nodes; which refers to situation that a true node marked as malicious node.

In order to overcome these challenges, in this paper, we proposed a new approach to detect all cooperative malicious nodes in a path. In the proposed scheme each node maintains trust value for its neighbor node. In MANET by using AODV protocol, before packet broadcast process compute the trust value, based on trust value compute the route trust and update the trust value in the routing table of the node. If the route is valid route then select most trusted node route then transmit the packets else compute the trust route for the exacting packet transmission.

2. RELATED WORK

Sankaranarayanan et al., [5] proposed security issues in MANET, detecting black hole attack by assigning fidelity levels to the participating nodes. The packet receiving ration is better than AODV in presence of cooperative black hole attack.

Sukant et al., [18] described the malicious attacked performance; isolation of malicious node, detection of malicious node will stop sending fake request call. It has been made to find impact of malicious node in AODV routing protocol under different malicious attack, the throughput and packet delivery ratio of normal AODV is much better than malicious attack AODV.

Valarmozhi et al., [3] measures the network performance based on number of nodes and number of hopes in the network, to increase the network capacity use multiple channel or radios per node with higher transmission speed.

Srinivas et al [10] proposed fuzzy based trusted and routing protocols using two parameters to categories the healthy and malicious node such as time ratio between route reply time and tome to live and dropped packet.

Radhakrishna Bar et al [13] calculated trust value based on packet forwarding ability and weight factor. The weight factor of a node is the ratio between RREQ received and RREP sent. In AODV protocol during packet transmission less trusted node can be avoided.

Asma Begam et al., [13] discussed in wireless sensor network black attack solution based on lightweight, efficient, fast and mobile agent technology. Proposed to defend against black hole attack using mobile agent in multiple base stations.

Marchang et al[11] proposed trust value to adopt every neighbor node, the neighbor node contains three structures like source list, To forward and forwarded.

Gayatri et al., [19] discussed selective forwarding attack. Efficient packet transfer between source to destination using Fuzzy theory and detect the attack using more challenging scenario.

Hai Xia et al [12] proposed trust based source routing to find the optimal route for secure routing. This method has four major parts route discovery, trust estimation, route update and route maintenance. Trust estimated the difference between the node's current trust and node's historical trust. The routing path is chosen based on minimal trust value.

Saparna Biswas et al[14] trust evaluated based on reliability, battery power and stability factor of node. Reliability of node drops to 0 then the node is malicious node, battery power considered certain time and stability includes two parameters pause time and velocity of node.

Payal et al., [6] described effective way of providing security in AODV against black hole attack, it detects malicious node by sending ALARM packets to its neighbors.

Yaser et al., [9] discussed black hole attack in ad hoc network. Before send the data packets trust table protocol modifies the behavior of the original AODV. The protocol reduces the bad affects of the black hole problem.

2. PROPOSED SCHEME

In this section we propose selection of most secure and reliable route by implementing the trust value management between two nodes with fuzzy logic rule forecast method. In the proposed scheme each node maintains trust value for its neighbor node. In MANET by using AODV protocol, before packet broadcast process compute the trust value, based on trust value compute the route trust and update the trust value in the routing table of the node. If the route is valid route then select most trusted node route then broadcast the packets else compute the trust route for the particular packet transmission.

The trust value calculated as

$$Ti(j) = \alpha Ti(self)(j) + \beta Ti(neighbor)(j) \text{ --- } 1$$

Where Ti(j) is the trust of node i on neighbor node j. Ti(self)(j) represent the trust value of node i on node j. Ti(neighbor)(j) represent the trust that neighbor of node I has on node j,and α, β are weighting factor that is $\alpha + \beta = 1$.

The neighbor node establishes three structures like to forward and forwarded and source list. To forward store the number of packet to be forwarded and forwarded store the number of packet that are already forwarded and source list define the progenitor of the packet to be forwarded. To forward count of node j is incremented by one when node i find that node j has received the packets which is to be forwarded further. Forwarded count is incremented by one when node j has forwarded that packet which is received.

During the packet transmission process the algorithm is, Immoral node maintain the source list(S_List) and observe the source packet.

If [(Forwarded) node j and (S_List Contains Immoral node)]

(Forwarded) node j++;

(ToForward) node j++;

(Forwarded) node j ≥ Limit

Else

Calculate the trust value again.

If morally wrong node fails to update forwarded and To Forwarded count of node j then detect as a malicious node else secure transmission.

3.1 Energy Auditor

In MANET the nodes energy is overwhelming when receiving and forwarding data to neighbor nodes. Initially all the nodes have full battery ability with maximum energy. According to energy use the selfish nodes utilize less energy because they only receive data packets they won't forward data packets to neighbors. Whereas the trusted node overwhelming more energy because they will receive and forward the packets to its neighbors. Each node has different energy calculation based on initial node pattern. The configuration requires following parameters when it's configuring like receive power consumption, transmission power consumption, ideal power consumption. In MANET energy consumption monitored by energy supervisor (EA) for each node when sending and receiving data packets to neighbor. Generally all nodes behave selfish to save battery power without forwarding the packets to the neighbor due to limited resource availability. Energy supervisor monitor packets received by a node, forwarded by a node and battery power affects by each node.

$$EA = \Sigma \text{ (Packet received + Packet forwarded + Batter power) / Node}$$

3.2 Trust Manager

Trust value intended by direct observation of neighbors. In the network every node monitors the behaviour of its neighbors. Every node monitors its neighbor node by using watch dog mechanism whether neighbor node really forward or drop the packets. The neighbor node is monitored by passively observing communication for detecting delayed packet, dropped packet and forward packets. These observations are abnormal action of any node and detect directly to determine the trust value. When communication begins the total trust value (TV) calculated with node index and direct trust value and stored in trust table for each node.

$$TV = \text{Node index} + \text{Direct trust}$$

The recommended trust obtaining indirect trust on Destination (D) from Node (N).

1. Node Source (S) sends Recommendation Trust Request to node(s) N.
2. If S has direct trust value on D, then it will reply back with Recommendation Trust Reply.
3. Else If S does not have direct trust value record it will discard the Recommendation Trust Request
4. After receiving Recommendation Trust Reply from neighbors consider the trust value of the node with maximum direct trust value by applying fuzzy logic technique.
5. Integrate all the obtained trust value from neighbors to calculate the indirect trust value

3.3 Packet Veracity Check

To maintain the integrity of the packet communication the modified message by the intermediate node can be discarded. Initially the packet veracity check value (PVC value) is positive. If any modification then PVC value will be decreased. Each communication generated by a node includes digital signature through its private key. Based on cryptography technique when a node receives a message decrypt using digital signature and public key to validate message from neighbor node. Similarly all the intermediate nodes authenticate the message and forward to the neighbor, if any modification in the message content then PVC value will be decremented. In our proposed scheme compared to other asymmetric key algorithms, RSA algorithm is implemented to perform digital signature verification and incur least cost.

3.4 Final Trust Manager

Final trust value of purpose node is calculated with energy value, trust value and packet veracity check value. These values are assigned by each node and generate node trust table for each node. The table contains Node ID, Trust value, Trust type and Trust

timeout. The centralized authority node request the final trust manager to recompute the trust value, the trust value of the node gets expired. Every time node trust table updated when ever final trust manager computing trust value. The final trust value is calculated as

FTValue = Evalue + Tvalue + PVCvalue

3.5 Certificate Authority

Any node with maximum trust value is elected as certificate authority node. Final trust table helps to certificate authority to obtain the trust value of each node. Based on certificate authority only the network ensures the secure transmission and separate the node with in time. Our value node get certificate from certified authority else node have to be renewed again. When centralized authority moves out of range then the next utmost trust value elected as a centralized authority node.

Source and destination nodes are certified by centralized authority, and then it is eligible for packet transmission. The packet is encrypted using public key from source node and forwards it to the destination. In between packet broadcast the intermediate node cannot decrypt and view the message only, the destination node can decrypt the packet using private key and view the message. In the proposed scheme MD4 algorithm used to hash the packet because it is least complex and incurs least energy cost.

ISAKMP secure transmission started before the actual transmission between the source and destination node. Source node send request to certified authority node, this certified authority node encrypt it with shared key SKs. After receiving this request certified authority node verifies whether the source and destination nodes are valid and also verify whether the destination in its range. Certified authority nodes generate CERTA and CERTB encrypt with shared key SKs, SKd and forward to source and destination node. Both source and destination node decrypt CERTA and CERTB, make authentication and start communication if certificates are valid.

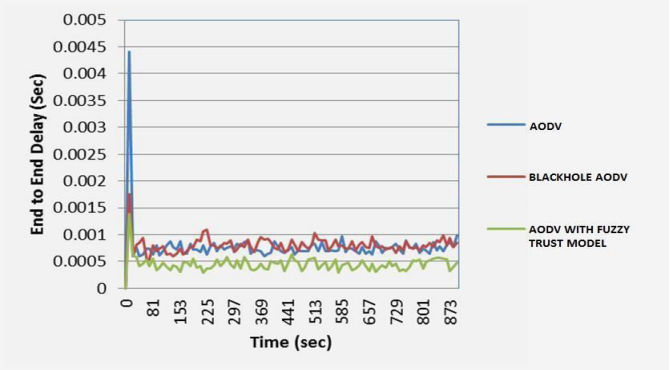
3.6 Fuzzy based analyzer

Node reliability increases its trust level, when trust level represents positive experience and node reliability decreases, when trust level represents negative experience. Fuzzy logic has trust values ranging between 0 and 1. The trust values of node can be calculated based on the computed Ev, Tv, PVCv and FTv. These values are the fuzzy input value and node mark as trusted node or malicious node based on fuzzy logic algorithm. When node establishes message to exchange packet data then fuzzy logic algorithm called automatically. If the fuzzy values falls below a critical threshold value then node marked as malicious.

When communication initializes between two nodes, source node sends request to certified authority for certify the node trust value, now fuzzy analyzer is invoked. Fuzzy analyzer verifies the trust level of source node and perform fuzzy table based on fuzzy analyzer algorithm. Certified authority determines the node is TRUSTED or MALICIOUS based on trust value. Certified authority find the requesting node as hateful then generate ALARM message and send to the entire trusted node in its range. Requester node is trusted the certificate authority to generate certificate based on fuzzy based analyzer and sends to the request node. Node makes secure broadcast when fuzzy values are VERY HIGH, HIGH and MEDIUM. Node fuzzy values are LOW and VERY LOW is marked as malicious node, certified authority denies certificate for hateful node in the network. When node certificate expired issued by the certificate authority, then trust node send request for renewal of credential before it starts transmission.

4. RESULTS AND DISCUSSIONS

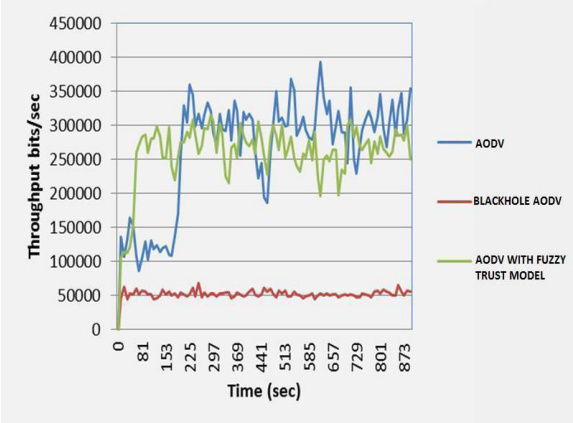
4.1End to End Delay



In figure. 1. The average time taken from CBR source to CBR destination by each data packet. Count only the

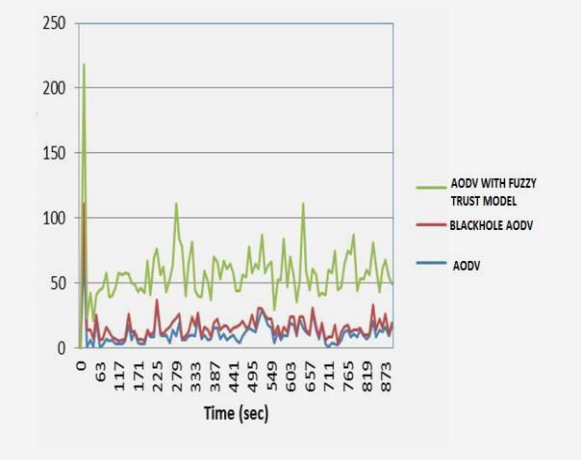
data packets that productively delivered. Time second increases black hole AODV end to end delay is high contrast to normal AODV. When apply AODV with fuzzy trust model the end to end delay is less contrast to both normal AODV and black hole attack AODV.

4.2 Through put



In figure.2. shows the throughput in bits per second, it is observed that the normal AODV the average throughput approximately 3,00,000 bits / second but in the black hole attacked the average throughput is 50,000 bits / second and AODV with fuzzy trust model the average throughput approximately reaches 3,00,000 bits / second. It shows that the normal AODV and fuzzy trust model throughput are almost same in the data transmission. The ratio between number of data packets received by the destination and number of data packets sends by source called packet delivery ratio.

4.3Packet delivery ratio



In figure. 3. The black hole attacked AODV is increased compare to normal AODV and AODV fuzzy trust model packet delivery ratio is high compare to both the normal AODV and black hole attacked AODV. This shows the fuzzy trust model make more packet delivery ratio. Though the packet delivery ratio is higher in proposed routing, end to end delay is less and throughput is significantly improved by the proposed trust routing.

5. CONCLUSION

In this paper, we focus on black hole security attack based on faith metrics and fuzzy logic and avoid black hole attack during route discovery. Normally AODV protocol is exaggerated due to selfish node, which results in low throughput and less end to end delay. Fuzzy trust model proposed to detect the black hole attack in AODV protocol. NS 2.35 simulation used to simulate the MANET and experiment the performance of throughput, end to end delay and packet delivery ratio. The experimental setup of proposed fuzzy trust scheme gives better throughput, less end to end delay and important packet delivery ratio. In Future research work includes analysis of all other routing protocols and compares the efficiency by identifying the malicious node and all the other possible attacks will be identified with new proposing model. This framework may extends to other scenarios like PAN, Emergency operation etc.,

REFERENCES

[1] V. Manoj, Mohammed Aaqib, N. Raghavendiran, R. Vijayan, " A Novel Security Framework Using Trust and Fuzzy Logic in MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3, No.1, January, 2012.

[2] J. Ramkumar, R. Murugeswari, "Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Special Issue 3, March 2014.

[3] A.Valarmozhi, M.Subala, V.Muthu "Survey of Wireless Mesh Network" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012.

[4] Shailender Gupta, C. K. Nagpal and Charu Singla, Impact of Selfish Node Concentration in Manets, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[5] Latha Tamilselvan, Dr. V.Sankaranarayanan ”Prevention of Co-operative Black Hole Attack in MANET” JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

[6] Payal N. Raj and Prashant B. Swadesh “DPRAODV: A Dynamic Learning System against Black hole attack in AODV based MANET “, International Journal of Computer Science, Vol. 2.S. (2009).

[7] Charles E. Perkins and Elizabeth M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In Charles E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000.

[8] Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma, Performance analysis of AODV, DSR & TORA Routing Protocols, IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010.

[9] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein,” A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks” International Journal of Communication Networks and Information Security (IJCNIS),2011.

[10] Sethi, Srinivas, and Siba K. Udgata, "Fuzzy-based trusted ant routing (FTAR) protocol in mobile ad hoc networks", Multi-disciplinary Trends in Artificial Intelligence, Springer Berlin Heidelberg, Pp. 112-123, 2011.

[11] Marchang, Ningrinla, and Raja Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", Information Security, IET 6, no. 2, Pp. 77-83, 2012.

[12] Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks 11, no. 7, Pp. 2096-2114, 2013.

[13] Bar, Radha Krishna, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh, "QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack", Procedia Technology 10, 530-537, 2013.

[14] Biswas, Suparna, Tanumoy Nag, and Sarmistha Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET", In Applications and Innovations in Mobile Computing (AIMoC), IEEE, Pp. 157-164, 2014.

[15] Akanksha Saini, Harish Kumar “Comparison between various Black hole Detection techniques in MANET” NCCI 2010 - National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, March 2010.

[16] Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M.”Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent” International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) July 15-16, 2012 Singapore.

[17] S. Sen, J.A. Clark - Guide to Wireless Ad Hoc Networks; In: Chapter 17-Intrusion Detection in Mobile Ad Hoc Networks-Springer, 2008. [11]. P. Brutch and C. Ko, “Challenges in Intrusion Detection for Wireless Ad-hoc Networks," In Proceedings of 2003 Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

[18] Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo” Detecting and Isolating Malicious Node in AODV Routing Algorithm “International Journal of Computer Applications (0975 – 8887) March 2013.

[19] V.Gayatri, C .Gomathi “Electing Monitoring node through Fuzzy Theory in Wireless Mesh Network for defense against selective Forwarding Attack” International Journal of Communications and Engineering Volume 02– No.2, Issue: 02 March2012.

[20] Timothy J.Ross Mcgraw Hill, Inc, ”Fuzzy Logic with Engineering applications“ [15]. A. Baddache, A. Belmehdi, “Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks,” International Journal of Computer Science and Information Security (IJCSIS). USA, vol. 7, iss. 1, pp. 10-16, January 2010.

[21] W. J. Adams, G. C. Hadjichristofi and N. J. Davis, “Calculating a Node’s Reputation in a Mobile Ad Hoc Network,” Proc. 24th IEEE Int’l Performance Computing and Communications Conference, Phoenix, AX, 7-9 April 2005, pp. 303-307.

[22] M. Imani, M.E. Rajabi, M. Taheri, M. Naderi, “Vulnerabilities in network layer at WMN”, International Conference on Educational and Networking Technology China, pp. 487-492, June 2010

[23] Gnanamurthy. R. K, Malathi. L, 2012, “A novel routing protocol with lifetime maximizing clustering algorithm for WSNIndia Conference (INDICON), 2012 Annual IEEE925-930.

[24] Gnanamurthy. R. K, Babyvennila. V and Bhuvaneswari. B, 2012, “Wireless sensor network for forest fire sensing and detection in tamilnadu”, Engineering Science and Technology: An International Journal (ESTIJ) Volume 2 Issue 2 Pages 306-309.