I. J. Computer Network and Information Security, **2018, 8, 51-57**
Published Online August 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.08.06

Implementing Security Features in MANET Routing Protocols

Abhishek Vyas
Vellore Institute of Technology, School of Computer Science & Engineering, Vellore, 603214, India
E-mail: abhishek.vyas2016@vitstudent.ac.in, abhishek_vyas@msn.com

Dr. Satheesh A.
Vellore Institute of Technology, School of Computer Science & Engineering, Vellore, 632014, India
E-mail: satheesh.abimannan@vit.ac.in

Received: 01 April 2018; Accepted: 22 June 2018; Published: 08 August 2018

Abstract—Mobile ad-hoc network or MANET is an auto-organizing network of mobile nodes. It lacks centralized control and is connected by wireless links. One of the many benefits of MANETs is that it can be utilized where there is no proper infrastructural support for wireless access and wired backbone is not possible. One major drawbacks of MANET is that as it is an infracture-less network, created on the fly, so here each node also functions as a router. So, each node participates in the routing of packets and information along the network. Due to this feature in MANETs, it is convenient to attack one of the nodes of MANET and then organize an attack on the whole network. To, secure the routing protocols in MANETs there are already a number of security features included in many of the unicast and multicast routing protocols. Like the use of unique signature and the use of secured algorithmic approach to secure against the various network layer routing attacks in MANETs. In this paper it is proposed that the use of hashing and secured algorithmic approaches like, Alpha Numeric Routing, when combined can introduce a unique security feature to On-Demand Routing protocols both in its multicast and unicast avatars. Some comparison, is done in the end of the new approach combines with the existing approaches by only using, Alpha Numeric Reflex Routing Algorithm. The outcome of the implementation was as expected, the results satisfied the input algorithms. Last but not the least analysis of the results is done and there is a discussion about the obtained results.

Index Terms—MANETs (Mobile Ad-hoc Networks), AODV (Ad-hoc On Demand Distance Vector Routing), SAODV (Secure Ad-hoc On Demand Distance Vector Routing), Secure Routing, Blackhole Attack, Wormhole Attack, Greyhole Attack, Java, JSIM (Java Based Simulation), Nodes, MiTM (Man in the Middle Attack).

I. Introduction

Last few years have been instrumental in the growth and implementation of wireless and mobile communication networks. Mobile ad hoc networks is a network which consists of nodes that are independent, form their topologies dynamically and use the wireless medium to communicate. One of the basic characteristic of MANET is that it is an infrastructure less network, so there is an absence of specified nodes for operations related to network management, as there are in the normal routers in the fixed and wired networks. For the maintenance of connectivity all the participating nodes in a MANET have to also route traffic in a network. The nodes cannot be dictated to cooperate by a central administrative authority as there is no such authority in the case of MANETs. Thus, a network-layer protocol that is designed for self- configuring networks should have rules that are enforced for connectivity and security requirements to make sure that the higher layer protocols are operating at an optimum level.[1]

Sadly the scenario is that most often used ad-hoc routing protocols have almost no security considerations and they blindly trust all the MANET participants to forward routing and data traffic in a correct manner. The above mentioned assumption sometimes proves disastrous for a mobile ad hoc network that trusts blindly its intermediate nodes for packet forwarding. "Some simulations have shown that if 10% to 40% of the nodes that participate in a mobile ad hoc network perform deceptive operations, then the average throughput degradation reaches 16% to 32%."[2] This paper presents a study and implementation details of the solutions that address the some problems of secure and robust routing in MANETs.

These are the attacks that a malicious node can use for disrupting the operation of a routing protocol in a self-configuring network like MANET. Here, an analysis of an already proposed secure ad hoc routing protocol that exist in the literature and its operational principles are presented in a scientific manner. This paper also shows the implementation of Alpha-Numeric routing algorithm and the use and integration of hashing algorithms in the Alpha-Numeric routing schemes to prevent any attacks on MANETS. [2] The latter is a novel approach taken in this paper as far as implementation of security of a routing protocol in MANET goes.

Routing protocols are a necessary evil in MANETs. They are responsible for identifying optimal route from a source node to a destination node in a particular MANET. One can classify routing protocols as reactive, proactive and hybrid routing protocols. For example, AODV: a reactive routing protocol, DSDV: a proactive routing protocol & ZRF: a hybrid routing protocol. The reactive routing protocol works in such a way, that when a route is not defined, it finds a route. Here, a source mobile node transfers *t* packets to a destination mobile node. Reactive routing protocol has to find the best route for the packets to reach destination node. In reactive routing protocols a route is found whenever it is needed, and maintenance of route is done if there is a link breakage. On the other hand in proactive routing protocols, each mobile node of MANET, has to maintain a routing table that should contain information about MANET's network topology and structure. Here, when the changes occur in any routing table they are periodically updated. Proactive routing protocols are not viable for the systems with huge number of mobile nodes. Here, to maintain the correct and updated information about routes, each mobile node sends control messages instant by instant. All mobile nodes broadcasts routing info to their neighbourhood mobile nodes. All nodes maintain routing table that possess the records of the nearby nodes and available nodes & the number of hops. [3]

Let's discuss about some of the security aspects of MANETs. In wired networks, security is implemented in three complementary stages viz., first prevention, and then detection and then if possible cure. The key to prevention state are the processes of authentication and authorization. The main concern of authentication stage is to authenticate the node that is participating, the message carried forward by the node, and meta-data like topology of the network and hop count etc. "Authorization process is intimately associated with recognition. Detection is defined as the ability to notice some anomalous behaviour from a node in the network. While, cure is defined as the ability to mitigate the effects of the anomalous behaviour of the node." [1]

Some possible attacks that are carried out on MANETs are eavesdropping on a node, compromising a node, distortion of messages relayed by a node, reply of messages by a node, failure to forward messages from a node, jamming of MANET radio frequency signals etc. The main issues that are responsible for the possible attacks and any security lapse in MANETs are confidentiality, authentication, availability, integrity, nonrepudiation and trustworthiness. [1]

The basic mobile ad-hoc networks depend on some fixed accesses point or other mobile node (in case of MANETs) for communication via sending and capturing packets. When one compares wired ad-hoc networks with MANETs, wired networks have a proper infrastructural set up for sending, forwarding, and capturing packets. While, MANETs are infrastructure-less and are open, so both authorized users and even hackers can easily access them with little or no effort. In MANETs there is no proper network management setup to monitor network traffic and its accessibility, this leads to attacks on MANETs from third parties like hackers, crackers and other malicious users. This paper focuses on the MANET's security mechanism, and pros and cons of some MANET protocols are discussed. The main focus of this paper is to show that, how a tiny novel approach of including hashing algorithm like SHA3 can enhance security and reliability in MANETs.[1]

The scope of securing MANETs is as follows, but it is not limited to these approaches:

- The ability to secure MANET conclusively is a massive task, due to its open nature and due to the absence of proper network management and infrastructure.
- Some previous implementations of MANET routing protocol security were not effective, in this ever changing world with new developments in technologies.[1]
- In MANETs, numerous layers are susceptible to attack, for example, MiTM attack is a multilayer attack.
- An intelligent approach for a comprehensive security of MANET has not yet been discovered.
- In this research, the focus is on the implementation of a secure routing scheme to prevent a routing attack by embedding SHA3 in the implemented secure routing protocol algorithm.

The main goal of this research paper is to provide enhanced security mechanism for the existing secure routing algorithm to prevent network layer attacks like wormhole attack etc. Also, to use the SHA3 (256 and 512) to enhance security in the existing secure routing algorithm. Here, there will also be an analysis of the above techniques with their implementation and comparison with the existing system.

Some applications that can be thought of the proposed implementations can be:

- A study of the system in relation to other systems, using parameters like the disappearance of packets, delivery rate of packets, and connectivity.
- A better knowledge of the QoS parameters, so that this misunderstanding can be used to solve various complex MANET network security problems.[1]

II. Proposed Scenarios & Methodology for Solving Wormwhole Routing Attack In Manets

Let us first start with a pictorial depiction and scenario for wormhole attack. In this type of attack in MANETs, two nodes are colluding together with each other to build a tunnel, in between the two nodes for sending and capturing the packets. They claim to other nodes in the MANET that they are providing the least distance path between the source and the destination nodes, in this manner they take full control of the other nodes in the MANET, this attack is only visible in the network layer

and not visible in the upper layers.[1].

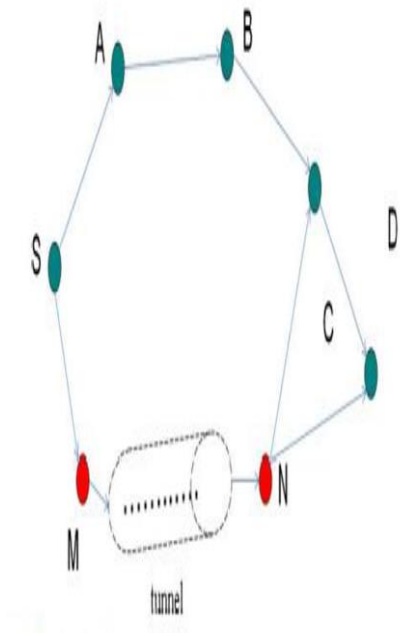

Fig.1. Scenario for Wormhole Attack.

"The Fig.1, above represents the wormhole attack situation. Here, *S* is the source node and *D* is the destination node. *A, B, C* are the connecting nodes, that are providing a path between the source and the destination. *M* and *N* here are the mischievous colluding nodes, tunnelling all the information and executing wormhole attack"[1]

The existing technique for preventing the wormhole attacks in MANETs is called Location based Geo and Forwarding (LGF) Routing Protocol.

To summarize LGF routing protocol, here the source node multicasts the RREQ message to all the intermediate nodes which contain the IP address of the destination node, based on the distance of the destination node.

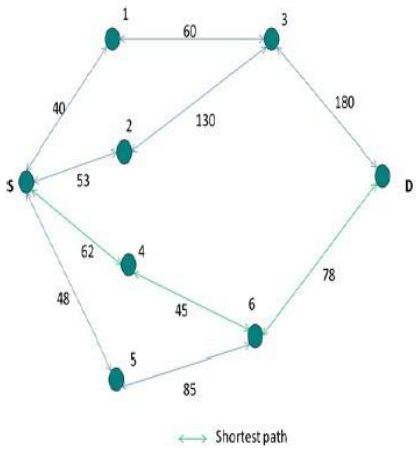

Fig.2. Schematic Diagram Showing LGF Protocol Implementation as Per Scenario Discussed Above for Mitigating Wormhole attack scenario.

The protocol is tested with source node 100 meters away from the destination node and the distance between the intermediate nodes is calculated by using the Clutter Formation of nodes in MANETs. This is same as the Pythagorean Distance Formula, i.e., $d = \sqrt{(n^2 - m^2) + (n'^2 + m'^2)} - (1)$ here, m, n, n', m' are nodes in the MANET topology which is clustered.

Now, the LGF protocol, does not necessarily solve the problem of the wormhole attack every time it is implemented in MANETs to turn around the effects of wormhole attack. The meaning is that LGF protocol is not 100 % secure, and cannot protect MANET from wormhole attacks all the time.

That is why, this paper tries to implement a secure routing protocol for MANET to prevent the effects of wormhole attacks. Here in this paper two unique methodologies are combined and a unique but novel approach to solving the wormhole attack problem in MANETs is proposed.

This paper uses the SHA-3 (min size 512 bits) algorithm and combines it with the Alpha-Numeric Routing Scheme to give a unique and novel approach to solving the wormhole attack scenario in MANETs.

For implementation purposes, JAVA based simulation tools were used. These tools used JSIM library themselves, this is a special library with specific functions for network simulation and ad-hoc network simulations. The simulation tool used was Dynamic Ad-Hoc Routing Simulator, it was implemented using JAVA and JSIM.

Some features of JSIM are the following:

- It is an object oriented library for the discrete time processes oriented simulation.
- Its main application area is queuing network simulations, however the range of its use can be very wide almost any system where object states changes discreetly can be modelled using JSIM.
- JSIM is a Simula like simulation environment written in JAVA.
- JSIM is built upon some very well-known principles inherited from the Simula language.
- As JSIM is completely written in JAVA so it is 100% portable. To run a JSIM application all one needs is latest JRE installed in one's machine.

Basically, the implementation algorithm here, uses SHA-3 to hash the values of common identifiers found via Alpha Numeric Routing Scheme. This way any intermediate node could not be approached by the malicious nodes, which form the tunnel in the wormhole attack scenario, thus preventing the wormhole attack altogether. This novel approach, does not let the intermediates nodes fall into the trap of malicious nodes that create the wormhole tunnel. This proposed approach when tested in simulation environment works almost 90%-95% of the time depending upon the input parameters.

The following input parameters are used in the implementation of the proposed methodology/algorithm to solve the wormhole attack situation in MANETs.

Table 1. Input Parameters for the Proposed Simulation

SIMULATOR USED	J-SIM Based Dynamic Ad-Hoc Routing Simulator
ROUTING PROTOCOL	ADOV
ATTACK SCENARIO	Worm-Hole Attack Prevention Implementation
Topology	1300 x 300 (meter square)
No# of Nodes Used	11
No# of Malicious Nodes	2 (They are the Worm Hole Creators)
Transmission Range	500 meters
Total Simulation Time	200 seconds
Movement Model	Random Waypoint Movement Model
Data Rate	0.25, 0.5
Traffic Agent	Constant Bit Rate i.e. CBR
Maximum Connections	All nodes are send at different times as per proposed algorithm.

So, basically the proposed architecture and the proposed novel secure routing algorithm's implementation, makes the probability of any misbehaving node to tunnel between the Source(S) and Destination node to almost zero. Due to the reason that it is not included in any of the groups of Alpha Numeric Routing. The packets transferred using the proposed algorithm safely, securely and efficiently reach the destination node (D).

III. Proposed Algorithm and Implementation Requirements

A. Hardware and Software Requirements

- Intel or any other processor with a minimum of 2 GHz processing speed
- RAM 256 MB or above
- Hard Disk Capacity 2 GB or more.
- Windows 7 Home or Higher version
- JRE 1.7 or higher and JDK 1.7 or higher version
- NETBEANS or ECLIPSE IDE installed in the system for implementation only.
- Dynamic Ad-Hoc routing Simulator - created using JSIM and SWING JAVA libraries. Purely JAVA based tool. Implemented in pure JAVA.

B. Pseudo Code for Proposed Algorithm – Alpha Numeric Reflex Routing Scheme Combined with SHA-3 (512 bits) Algorithm.

ALGORITHM: ALPHA-NUMERIC_SHA-3

Start of Algorithm Pseudo Code

Node Initialization in the MANET
Source and Destination node initialization

```
for i:= 0 to n do this
        Ln(i) ← nodes with high power attribution with an ability to manage other nodes.

        if(nodes are in range of Ln)
           then (apply the SHA-3 algorithm)
                // SHA3 gives hash value
           transmit the common identifier
        else
           node is other than Ln
        end if
end for

for i = 0 to n do this
        for j = j +1 to n do
                An(i, j) ← nodes receive common identifier from other Ln

                        if(nodes accepts the common identifier and accepts its details to Ln) then
                        node:= trusted
                        else
                        node:= malicious
                        end if

    Now Apply SHA-3 on the Source Node (S)

        Source Node→Forward RREQ packets

                if (Source node and Destination Node are under the same Ln) then

                Forward RREQ →Destination Node (D)
        Match the SHA signature for verifying the authenticity of the information carried by the node.

                 else
                 Forward RREQ →An(i,j)

                An(i,j) → Ln(i)
                Ln(i) → Destination Node (D)
    Match the SHA signature for verifying the authenticity of the information carried by the node.
                end if

        end for

end for
```

End of Algorithm Pseudo Code.

IV. Results and Discussion

A. Simulation Results

Here, this above figure shows that F and B are the two malicious nodes that have the potentiality to form a wormhole. Also the Source Node in this MANET structure is A and the Destination Node is I.

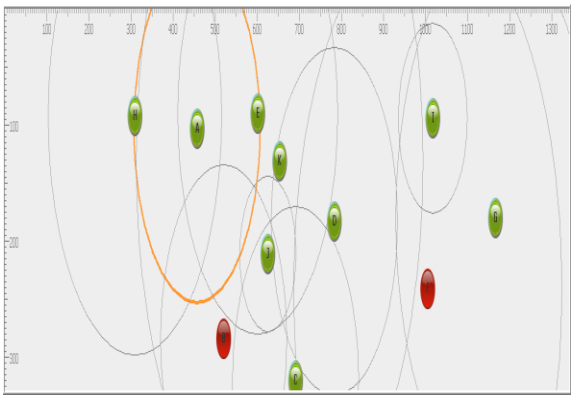

Fig.3.Simulation Results of the above the Implementation of the above Mentioned Proposed Pseudo Code

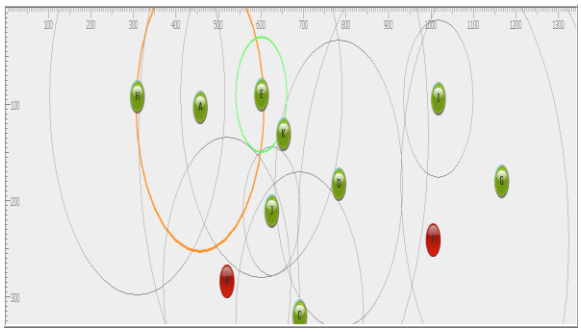

Fig.4. Simulation of Node A Transmitting into its Neighbouring nodes.

The above simulation in Fig.4. snapshot shows how node A is transmitting to its neighbouring nodes, and how the mechanism of transferring packets works in this simulation.

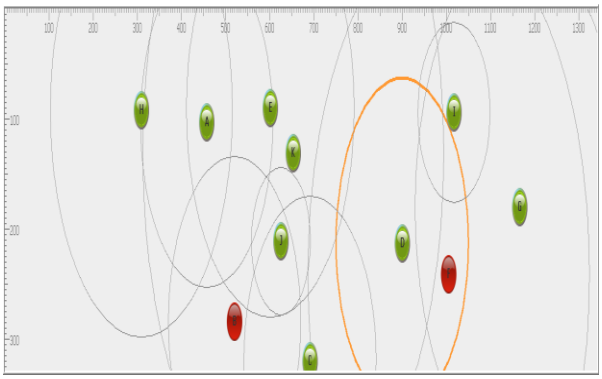

Fig.5. Simulation Snapshot showing Route Transference

The above simulation snapshot in Fig.5. shows route transference, with the simulation showing the shift in the route as indicated by the shift or movement of the orange circle in the simulation. This shows that the packets transferred between the nodes in the above MANET are trying to avoid the malicious nodes so that wormhole attack cannot be implemented.

This simulation (Fig.6.) snapshot shows the completion of the simulation with the transfer of the message (packets) from the source node A to the destination node I, the packets transferred bypassed the malicious nodes B and F and their malicious attempt to create a wormhole in the MANET network.

Fig.6. Completion of the Simulation

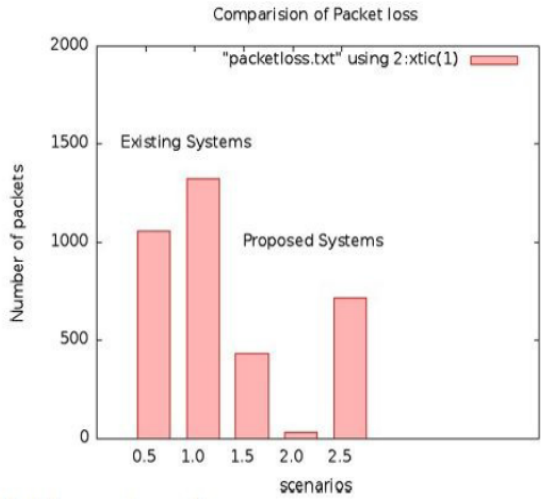

Fig.7. Comparison of the Packet Loss using the Existing Scheme and the Proposed Schemes.

The above Fig.7. shows the comparison that how many packets are lost using the existing schemes when compared to the unique novel scheme in this paper.

V. Conclusion

MANETs are facing vulnerabilities & security issues for a long time now. This research paper implements a secure routing algorithm with a scientific & efficient approach for optimization of the packet loss frequency & acknowledgement of receipt of packets and authentication based on SHA algorithm is proposed and implemented. The algorithmic approach for routing is implemented using Java Application for routing protocols to execute the scenarios and results. The benchmark algorithm for the testing of the proposed implementation was the criteria met by the LGF protocol. The proposed implemented algorithm had to exceed the output expectations of the LGF protocol. The final outcome of the implementation and the simulation of the unique application of the combination of SHA-3 and Alpha Numeric Routing Scheme is that, it protects the MANETs form the wormhole attack scenario almost 100% of the time. One can say that there can be further improvements related to implementation efficiency of the proposed algorithm can be made but all in all it's a robust and quite efficient algorithm for the security of MANETs against wormhole attacks.

The future of security in MANETs is the use of bio-inspired algorithms and swarm intelligence algorithms for routing protocols efficient functioning and security.

REFERENCES

[1] R. Singh, P. Singh and M. Duhan, "An Effective Implementation of security based algorithmic approach in mobile Adhoc networks.", Human-Centric Computing, Springer Open-Access Journal, E4:7 (2014). http://www.hcis-journal.com/content/4/1/7

[2] W.Chen Wu, H.Twu Liaw, "A study of High Secure and Efficient MANET Routing Scheme.", Journal of Sensors, Hindawi Publishing, Vol.1 (2015). http://dx.doi.org/10.1155/2015/365863

[3] R. Dilli, P. Chandra Sekhar Reddy, "Implementation of security features in MANETs using SHA-3 Standard Algorithm." ICCSISSS, Vol.1 (2016).

[4] R.K. Singh, P. Nand, "Literature Review of Routing Attacks in MANET", ICCCA, Vol.1 (2016).

[5] M.A. Abdelshafy, P. J. B King, "Analysis of security attacks on AODV routing", IEEE, E1:2, pp 290-295 (2013).

[6] Ratish J. Punnoose, Richard S. Tseng, and Daniel D. Stancil. Experimental results for interference between Bluetooth and IEEE 802.11b DSSS systems. IEEE Vehicular Society Conference, October 2001.

[7] Li JH, Das S, McAuley A, Lee J, Stuhrmann T, Gerla M (2010) A multi-layer approach for seamless soft handoff in mobile ad hoc networks. Hui Zeng Intell. Autom., Inc. (IAI), Rockville, MD, USA, pp 21–26, GLOBECOM Workshops (GC Wkshps), IEEE.

[8] M. Guerrero Zapata, "Key Management and Delayed Verification for Ad Hoc Networks," J. High Speed Networks, vol. 15, no. 1, Jan. 2006, pp. 93–109.

[9] M. Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," Proc. 1st ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[10] Cerri David, Ghioni Alessandro, "Securing AODV: The A-SADOV Secure Routing Prototype", Security in Mobile Ad Hoc and Sensor Networks, IEEE communication magazine, February 2008, pp. 120-125.

[11] X. Hong, K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks," IEEE Network, vol. 16, no. 4, July–Aug. 2002, pp. 11–21.

[12] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in Proceedings of the 2010 IEEE Symposium on Security and Privacy.

[13] Radha S. S, S. V. Dhopte "The Secure Dynamic Source Routing Protocol in MANET using MD5 Hash Function" HEIR Vol I, Issue 3, 2012 ISSN: 2277 – 5668.

[14] C Lee "A Study on Effective Hash Routing in MANETs" Advanced Science and Technology Letters Vol.95 (CIA 2015), pp.47-54.

[15] B Carbunar, C Nita-Rotaru "JANUS: A Framework for Scalable and Secure Routing in Hybrid Wireless Networks" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 6, NO. 4, OCT DEC 2009.

[16] Md. T Rahman, MdJ N Mahi "Proposal for SZRP Protocol with the Establishment of the Salted SHA-256 Bit HMAC PBKDF2 Advance Security System in a MANET" International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT) 2014.

[17] P. Papadimitratos and Z. J. Haas, "Securing the Internet Routing Infrastructure," IEEE Commun. Mag., vol. 10, no. 40, Oct. 2002, pp. 60–68.

[18] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," Proc. 6th Annual ACM/IEEE Int'l. Conf. Mobile Comp. and Net. (Mobicom'00), Boston, Massachusetts, Aug.2000, pp. 255–65.

[19] L.Buttyan, J.Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM Journal for Mobile Networks, Special Issue on Mobile Ad Hoc Networking, 2002.

[20] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, "A secure routing protocol for Ad-hoc networks," Proc. Of IEEE ICNP, 2002.

[21] Manel Guerrero Zapata and N. Asokan: "Securing Ad hoc Routing Protocols". In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pages 1-10. September 2002.

[22] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks", IEEE ISCC 2002.

[23] Tao Lin, "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications", Ph.D. Dissertation, Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.

[24] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, Security in Mobile Ad hoc Networks: Challenges and Solutions, IEEE Wireless Communications. February 2004. Adam Burg, "Seminar on Ad Hoc Network Specific Attacks".

[25] M. Ramkumar, N. Memon, KPI: A Security Infrastructure for Trusted Devices, Pre-Conference. Workshop, 12th Annual Network and Distributed System Security Symposium, San Diego, California, 2 February 2005.

Authors' Profiles

Abhishek Vyas is an Indian Citizen. He completed his Master of Technology degree in Computer Science and Engineering with specialization in Information Security in June 2018 from Vellore Institute of Technology, Vellore, Tamil Nadu, India. Previously, he completed his Bachelor of Technology in Computer Science and Engineering from Suresh Gyan Vihar University, Jaipur, Rajasthan, India in July 2016. He plans to pursue a Ph.D. in Computer Science and Engineering in the future.

Professor Dr. Satheesh A. also an Indian Citizen is an Associate Professor in the School of Computer Science and Engineering at Vellore Institute of Technology, Vellore, Tamil Nadu, India. He holds a Ph.D. in Computer Science and has many years of experience in teaching and research.

How to cite this paper: Abhishek Vyas, Satheesh A.,"Implementing Security Features in MANET Routing Protocols", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.8, pp.51-57, 2018.DOI: 10.5815/ijcnis.2018.08.06

