Academic City University College – Accra Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
Tony Blair Institute for Global Change
FAIR Forward – Artificial Intelligence for All - Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Accra Bespoke Multidisciplinary Innovations Conference (ABMIC)

& The Africa AI Stakeholders' Summit 14th December, 2021

Towards The Development of a Hybrid Routing Protocol for Flooding Attacks Mitigation in MANET

Abubakar M. Baba
Department of Computer Engineering, Kaduna Polytechnic, Kaduna, Nigeria
PhD candidate - Department of Computer Engineering, University of Benin City, Nigeria
E-mail: abubakarbm2020@gmail.com
Phone: +2348137436158

Simon T. Apeh
Department of Computer Engineering
University of Benin
Benin-City, Nigeria
Email: apeh@uniben.edu
Phone: +2348034956812

Kachikwu B. Erameh
Department of Computer Engineering
Kaduna Polytechnic, Kaduna, Nigeria
E-mail: Kachikwu.erameh@uniben.edu
Phone:+2347061694781

Proceedings Citation Format

Abubakar M. Baba, Simon, T. Aoeh & Kachikwu, B. Erameh (2021): Towards The Development Of A Hybrid Routing Protocol For Flooding Attacks Mitigation In MANET. Proceedings of the Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. December 2021. Pp 153-162 www.isteams.net/ghanabespoke2021. DOI https://doi.org/ 10.22624/AIMS/ABMIC2021P12

Towards The Development Of A Hybrid Routing Protocol For Flooding Attacks Mitigation In MANET

Abubakar M. Baba, Simon, T. Apeh & Kachikwu B. Erameh

ABSTRACT

Mobile Ad-Hoc Networks are infrastructure-less wireless communication technology that interconnects mobile devices such as phones, laptops, and smart devices including providing flexibility, seamless communication and mobility to all devices forming the network. MANET suffers security lapses due to the absence of central control infrastructure to monitor and control the devices that joins the network. These security lapses in MANET discourage it and makes it vulnerable to attacks such as denial of service attacks. Amongst various attacks prevalent on MANET environment, packet flooding is a common attack and causes a devastating effect on MANET nodes which if left undetected may lead to consequent crashing of the entire network. There is need to secure data and be kept confidential. In this paper, the separation of trusted nodes from malicious nodes and to protect the data packet from attackers is to be taken as research goal. Therefore, a highly secured Hybrid Trust-based Anonymous Authenticated Routing Protocol (HTBAARP) to mitigate flooding attacks is to be developed to avoid unauthorized access and to detect malicious nodes. This will be achieved by integrating a Modified Authenticated Anonymous Routing Protocol (MAASR) to a Trusted Management Scheme (TMS). Simulation will be done using NS-2 in conjunction with MATLAB R2020a to evaluate performance. The proposed solution is expected to improve throughput, packet delivery ratio and, reduces routing delay and routing overhead in the network.

Keywords*:* Anonymous, Flooding, Hybrid protocol, MANET, Malicious nodes, Routing

1. BACKGROUND OF STUDY

Wireless communication networks are broadly classified into infrastructure wireless network and infrastructure-less wireless networks where infrastructure wireless networks means that the communication established between nodes is control centrally while infrastructure-less means that communication between the network nodes is established through hop-to-hop and this type of networks is also referred to as ad hoc network (Abu Zant & Yasin, 2019) Connection between the neighbor nodes and the end user nodes does not rely on infrastructure to form network and nodes in the adhoc network depend on multi-hop to communicate with one another, therefore all the required services such as forwarding, maintenance, routing and administration are carried out by the nodes themselves (Sandeep & Rajesh, 2014). The use case of MANET is diverse and ever expanding, as more devices are made portable and wireless communication capable. However, the absence of central control infrastructure that affords MANET its flexibility and adaptability to different use scenarios is the main challenge when security and communication integrity is considered to be vital, like in the case of medical and military application (Gurung, 2017). In MANETs, there are different types of routing protocols

each of which is applied according to the network peculiarities (Dhenakaran & Parvathavarthini, 2013). According to Kumar & Kumar (2012),
A routing protocol is a standard that governs how nodes in a wireless domain decide how to route incoming packets between nodes (devices). Many different routing protocols for MANET have been developed over the years. These protocols are broadly classified into three types: proactive, reactive, and hybrid routing protocols (Abdulleh et al., 2015). Because of the challenges that MANETs pose to related protocols, it has become one of the most popular areas of research in recent years (Ankur & Prabhakar, 2013). The early routing protocols such as AODV mainly focused on how to route the data packet in MANET efficiently without considering the potential malicious node that may sneak or collet traffic information of the network (Wei, 2014). Thus, Considerable emphasis was given by researchers to develop an anonymous routing protocols that can improve MANET security (Paolo et al, 2017).

For a reliable communication and relationship between nodes in the network, nodes need to be logically trusted. To achieve it then researchers adopted a trust management process to manage the trust level of a node in M ANETs network. Trust management in MANETs is needed when participating nodes desired to established a network with an acceptable level of trust (Jin-Hee, 2010). These security lapses in MANET discourage its thereby limiting the immense advantages that it offers in terms of flexibility, adaptability and cost. The attacks in MANET are broadly classified into two, which are Passive and Active attacks.

In passive attacks, the attacker or attackers only gathers information about the network and other network nodes, without affecting the network operation or degrade network performance. Some of passive attacks are eavesdropping, traffic analysis and monitoring (Kumar et al, 2018). While in active attack, the aim of the attacker node is to affect the network performance, integrity and security by purposefully dropping, rerouting, modifying, losing, delaying packets in the network. Some of the common active attacks in MANET are Spoofing attack, Black-hole attack, Gray-hole attack and Flooding attack (Kumar et al, 2018). Amongst various attacks prevalent on MANET environment, packet flooding is a common attack and causes a devastating effect on MANET nodes which if left undetected may lead to consequent crashing of the entire network (Mallikarjuna & Anusha, 2020).

Active attacks are considered more threating and costly in MANET (Hajiheidari et al, 2019) compared to passive attacks, as the attacks leads to severe loss of network performance, degraded throughput and expend energy of legitimate nodes in the network thereby reducing overall network lifespan of the network . With the adoption of MANET technology in military application for fast and dependable communication in training and combat situation, civilian and paramilitary activities such as search-and-rescue operation, and other widespread use of MANET, the threat of active attacks especially flooding attack is considered capable of derailing these vital operations.

The remaining part of the paper is as follows: Section Two present the related works, Section Three proposes the methodology for achieving the aim. Section Four the expected outcome of the research, Section Five contains expected contribution to knowledge and conclusion.

1.1 Research Problem

Challenges associated with securing mobile adhoc networks (MANETs) due to flooding attacks include: inadequate provision of an authorized authentication of routing protocol that can detect and mitigate all the different types of flooding attacks. To the best of my knowledge, a lot of

research have shown that most of the existing approaches suffers from routing delay and routing overhead.
Most existing approaches or protocols do not integrate the mentioned security features which lead to vulnerability in MANET security system, also many researchers have made efforts towards improving security in MANET by modifying the conventional AODV routing protocol, and however most of the proposed solutions designed do not scrutinize the network packets in order to identify malicious or illegitimate packets. Hence, there is need for development of a robust system that will enhanced the performance of MANET network.

1.2 Research Thrust

The research study is intended towards the development of hybrid routing protocol for mitigation of flooding attack in MANET and will be achieved the following: by modifying an existing Authenticated Anonymous Secured Routing Protocol (AASR), develop and evaluate a trust-based management scheme, hybridize the trust-management scheme with the Modified Anonymous Authenticated Secured Routing Protocol, evaluate the performance of the developed hybrid routing protocol under flooding attacks in terms of delay and Packet overhead and lastly implement the developed protocol using a test-bed.

2. RELATED WORKS

What follows is a review of several researches carried out by researchers that has made contributions in the domain of study.

Gurung (2017) developed a novel approach for mitigating route request flooding attack in MANET. In the proposed approach, a mechanism referred to Mitigating Flooding Attack Mechanism (MFAM) was used to mitigate the effect of non-addressed spoofing attack. This mechanism, relied on the deployment of special nodes called F-IDS (Flooding – Intrusion Detection System), which are setup in sniff mode to detect traffic from neighbor nodes, analyze and interact with the other nodes in the network. The MFAM has three main phases, viz, Dynamic threshold computation, - during which the RREQ packet rate is set, Confirmation phase, - where the F-IDS confirm the rate the intent of a suspicious node to be either malicious or legitimate, then inform the entire network of the threat presence via an ALERT package, finally the Resetting phase, - the point where the malicious node restrictions are lifted and node status set to neutral. The mechanism is simulated using NS-2.35 software.

Also Vimal & Nigam (2017) proposed a flooding-based DDOS attack plummeting technique in MANET, using neighborhood nodes table. In the work presented by the authors, a computation of average node packet data is acquired during normal un-attacked operations, the average packet data is compared to under-attack packet situations. When the packets received from a particular node are found to be in excess of the average expected from legitimate nodes in the network, the suspicious malicious node is blacklisted by its neighbor node, and an Alarm message is sent to all other neighboring nodes around the suspected malicious node to update their routing table with the new information regarding the malicious node, thereby blacklisting the node and cutting it off the network. The result from the simulation carried out in NS-2 was reported to show improved PDR, throughput and reduced overhead.

Mallikarjuna and Anusha (2020) worked on an optimized and hybrid energy aware routing model for effective detection of flooding attacks in a MANET environment which has to do with the

feature extraction and a classification model based on ANFIS (Adaptive Neuro-Fuzzy Inference System). By using ANFIS classifier, the extracted feature was trained and then classified.
A security mobile agent (SMA) integrated with AODV protocol called security mobile agent-adhoc on demand routing protocol (SMA$_2$AODV) to detect flooding attacks for MANETs was developed. Ant Colony Optimization (ACO) and Fitness Distance Ratio Particle Swarm Optimization (FDR PSO) are used in combination with the routing protocol SMA$_2$AODV model in the work to prevent flooding attacks, ACO chooses an energy-efficient route and FDRPSO optimizes all nodes that are energy consumed. The hybrid ACO-FDR PSO optimization approach considered energy as its function of fitness. The performance metrics considered were analyzed using the NS-2 simulator with existing benchmark methods.

3. METHODOLOGY

3.1 Research Design

The design and development approach to be adopted in realizing each of the objectives of the research work and the steps needed to carry out each of the activity are outlined as follows:

1. To modify and evaluate the Authenticated Anonymous Secured Routing Protocol (MAASR) for Mobile Ad Hoc Network.
    a. Modify packet header for anonymous onion encryption.
    b. Generate public key size for each participating node in the network.
    c. Develop a source and intermediate node route request.
    d. Implement a destination node verification sequence.

2. Evaluate the performance of traditional AASR and the modified MAASR protocols under flooding attacks.
    a. Create a MANET scenario with multiple mobile nodes with all nodes legitimate
    b. Create a MANET scenario with multiple mobile nodes with malicious node.

3. Develop a trust-based management scheme for Mobile Ad Hoc Network
    a. Determine a trust value calculation algorithm via direct and indirect observation.
    b. Determine a trust threshold for node rejection and blacklisting.

4. Integrate the trust-management scheme with the Modified Anonymous Authenticated Secured Routing Protocol (MAASR) to obtain a hybrid routing protocol.
    a. Determine threshold for network delay and buffering to prevent incorrect node rejection and blacklisting.
    b. Compress and integrate encrypted anonymous authentication packets within the network for easy updating with trust management scheme.

5. Evaluate the performance of the developed routing protocol under flooding attacks in terms of Delay and Packet Overhead.
    a. Simulate the developed hybrid routing protocol under flooding attacks, measure and compare performance indices with non-hybrid routing protocol like AASR, MAASR and trust-based protocol alone.

3.2 The proposed Hybrid Protocol

After developing the proposed hybrid routing protocol by combining the anonymous secured routing protocol with trust management scheme which guarantees a secured MANET that can detect and mitigate DDOS attacks. Flooding attacks can be easily detected and mitigated without compromising network efficiency, speed or performance. This will be achieved by each RREQ packet public and private key encrypted before broadcast, while all receiving intermediate node first determine trust value of the sending node before processing the received packet, where low trust values lead to blacklisting of nodes until their status is dynamically updated as they change behavior. Packets from blacklisted nodes with low trust values are ignored by neighbor nodes to prevent flooding.

For nodes with high trust value, the neighbor nodes onion encrypts the packet and forwards it after failing decryption attempt with private, thereby determining the packet is not destined for it. The destination node successfully decrypts the sent packet, prepares and send RREP, which also undergoes same scrutiny and trust value verification at all intermediate nodes, and also onion encryption until the source node is reached, which forwards the data packet via the shortest possible established secured route. This guarantees anonymity and security within the network. A flowchart of the overall proposed Hybrid Trust-based Anonymous Authenticated routing protocol is presented in Figure 1.

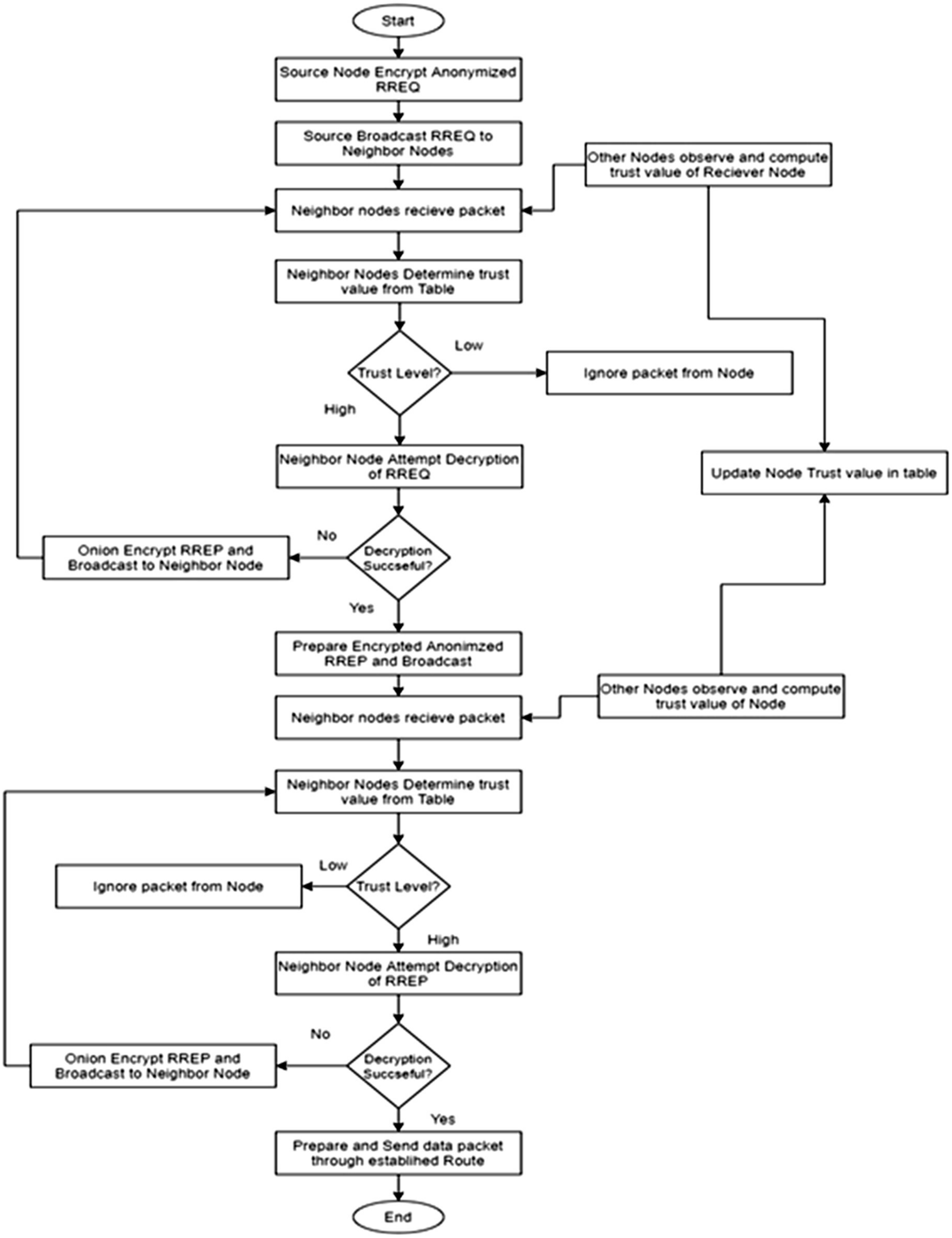
Start
Source Node Encrypt Anonymized RREQ
Source Broadcast RREQ to Neighbor Nodes
Other Nodes observe and compute trust value of Reciever Node
Neighbor nodes recieve packet
Neighbor Nodes Determine trust value from Table
Trust Level?
Low
Ignore packet from Node
High
Update Node Trust value in table
Neighbor Node Attempt Decryption of RREQ
No
Onion Encrypt RREP and Broadcast to Neighbor Node
Decryption Succseful?
Yes
Prepare Encrypted Anonimzed RREP and Broadcast
Other Nodes observe and compute trust value of Node
Neighbor nodes recieve packet
Neighbor Nodes Determine trust value from Table
Low
Ignore packet from Node
Trust Level?
High
Neighbor Node Attempt Decryption of RREP
No
Onion Encrypt RREP and Broadcast to Neighbor Node
Decryption Succseful?
Yes
Prepare and Send data packet through establihed Route
End

Figure 1: Flowchart of Proposed Hybrid Trust-based Anonymous Authenticated Routing Protocol (HTBAARP)

4. SIMULATION

The network simulation will be carried out in three different scenarios, first with the modified anonymous authenticated secured protocol (MAASR), with the trust management scheme (TSM) and lastly with hybrid protocol (HTBAARP) implemented. The simulation parameters are summarized in table 4.1.

Table 4.1: Simulation Parameters

PARAMETERS	VALUES
Simulation Software	
Matlab	Version R2020a
Network simulator	NS-2.35
Simulation Parameter	
Network Size	1 km^2
Number of Nodes	100
Number of malicious node	10
Network topology	Poisson Point Process
MANET mobility	Random way point model
Node Speed	20, (m/s)
Simulation time	1200 (s)
Position awareness	All nodes
Location of malicious Nodes	Network center (middle)
Antenna type	Omni-Directional
Transmission range	250 m
Wireless environment	MANET free space path loss model

5. DATA PRESENTATION

The data will be presented and analyzed in tabular forms as describe in Tables 5.1 and 5.2 respectively and the simulation result will be presented in graphical forms. After evaluating the performance of the existing Authenticated Anonymous Secured Routing Protocol (AASR), the modified Authenticated Anonymous Secured Routing Protocol (MAASR), the trust management scheme (TMS) and the propose Hybrid Trust-based Anonymous Authenticated Routing Protocol (HTBAARP) in terms of the selected metrics (throughput, delays, packet delivery ratio) against the number of nodes through simulation at different scenarios, each result obtained will be discussed according to the observed performances.

Table 5.1: Expected result analysis of MAASR

Number of Node (NN)	Time to Live (TTL)	Encryption Time (ET)	Decryption time (DT)	Number of Hops Count (NHC)

Table 5.2: Expected result analysis of TMS

Node identification (NI)	Trust value (TV)	Neighbor node trust value (NTV)	Trusted node (TN)	Blacklist node (BLN)

6. DISCUSSION OF FINDINGS

The discussion of our results will eventually be based on the observations obtained from the graph, which is the outcome of the simulation and the research work will be set up in a real life scenario using a communication enable hardware device called raspberry pi.

7. CONCLUSION

This research proposal presents a methodology to develop a hybrid routing protocol to improve security in MANET which is a serious challenge to deployment of the networking technology in high risk application like military and critical civilian infrastructure due to the severity of successful attacks like flooding, leading to denial of service scenarios. The hybrid routing protocol is proposed to be achieved by a combination of a Modified Anonymous Authentication Secured Routing Protocol and a Trust-Based Management Scheme to detect, mitigate and isolate malicious nodes, while reporting the status of the node and trust level across the network. This proposed scheme helps to improve the network security, while ensuring a low packet delivery delay across the network and also ensure a minimal packet overhead.

8. EXPECTED CONTRIBUTION TO KNOWLEDGE

In light of the literature review and study, this research work is envisaged to provide a comprehensive knowledge base for other researchers in the field of Mobile Ad-Hoc network (MANET) through the following:

1. A hybrid routing protocol for more secured communication in MANETs will be developed
2. The Proposed modification of AASR will be designed that is adaptable to other hybridization efforts which can be adopted by other research applications in communication such as Vehicular Ad-Hoc Network or Wireless Sensor Network.
3. An effective performance of the proposed solution will be evaluated for high malicious detection rate under RREQ flooding, Data flooding, Error flooding, hello flooding and SYN flooding.

REFERENCES

1. Abdulleh, M.N., Yussof, S. and Jassim, H. S. (2015). Comparative Study of Proactive, Reactive and Geographical MANET Routing Protocols. *Communications and Network*, pp. 125 -137. DOI: http://dx.doi.org/10.4236/cn.2015.72012.
2. Abu Zant, M., & Yasin, A. (2019). Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV). *Security Communication Networks,*
   Ankur, O. B. and Prabhakar, L. R. (2013). MANET: History, Challenges and Applications. International Journal of Application or Innovation in Engineering & Management (IJAIEM). (2) 9, ISSN 2319 – 4847.
3. Gurung, S. (2017). A novel approach for mitigating route request flooding attack in MANET. *Wireless Networks*. doi:10.1007/s11276-017-1515-0
4. Dhenakaran, S., & Parvathavarthini, A. (2013). An overview of routing protocols in mobile ad-hoc network. *International Journal of Advanced Research in Computer Science Software Engineering, 3*(2).
5. Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Journal of Computer Networks, 160*, 165-191.
6. Jin-Hee C., Ananthram S., & Ing- Ray C (2010) A survey on trust management for mobile Adhoc networks. IEEE Communication survey & Tutorials. pp. 1-22.
7. Kumar, S. and Kumar, J. (2012). Comparative analysis of proactive and reactive routing protocols in mobile ad-hoc networks (MANET): Journal of Information and Operations Management. ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, PP-92-95
8. Kumar, V. V., & Ramamoorthy, S. (2018). *Secure adhoc on-demand multipath distance vector routing in MANET.* Paper presented at the Proceedings of the International Conference on Computing and Communication Systems.
9. Mallikarjuna N & Anusha K (2020). An optimized and Hybrid Energy Aware Routing Model for Effective Detection of Flooding Attacks in MANET Enviroment, Research Square,VIT-university, Chennai, India.
10. Paolo P., Luca C., & Dario M. (2017). An Anonymous inter-networks Routing Protocol for the internet of Things, Journal of Cyber Security and Mobility. 6(2), 127-146.
11. Vimal, V., & Nigam, M. J. (2017). *Plummeting flood based distributed-DoS attack to upsurge networks performance in ad-hoc networks using neighborhood table technique.* Paper presented at the TENCON, IEEE Region 10 Conference.
12. Wei Y. (Anonymous Routing protocol with Authemticated key Establishment in wireless Ad Hoc Networks. international Journal of Distributed Sensor Networks. pp. 1-10 DOI: http://dx.doi.org/10.1155/2014/222350.
13. Sandeep, S., & Rajesh M. G (2014) A Cross Layer Approach for Intrusion Detection in MANETs, International Journal of Computer Applications Buddha University Greater Noida, India. 93(9), 0975 – 8887.