Anonymous Secure Routing Protocol for Multi hop Wireless Mesh Network (ASRP)

J. Srinivasan, S. Audithan

Abstract: Anonymous communications are important for many applications of the Wireless Mesh Networks (WMNs) deployed in adversary environments. A major requirement on the network is to provide unidentifiability and unlinkability for nodes and their traffics. The existing protocols are vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broad- casting, even the node identities are protected by pseudonyms. In this paper, we propose Anonymous Secure Routing Protocol for Multi hop Wireless Mesh Network (ASRP) to protect the attacks and multi hop secure data transmission in WMN. ASRP offers anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. The key-encrypted onion routing is designed to prevent intermediate nodes from inferring a real receiver node. Simulation results indicate that the efficiency of the proposed ASRP protocol with improved performance as compared to the existing protocols.

Keywords: Anonymous, Onion Routing, Encryption, Decryption, Wireless Mesh Networks.

I. INTRODUCTION

Wireless Mesh Network (WMN) is characterized as quick operation and self-organizing, multi-hop network. WMN has emerged as a capable technology to meet the challenges of the next generation wireless communication networks for provide adaptive, flexible, reconfigurable also present cost-effective industry solutions to the service providers. The possible applications of WMNs are high-speed wireless metropolitan area networks, community networking, intelligent transportation system networks, backhaul connectivity for cellular radio access networks, defense systems, building automation, and city-wide surveillance systems etc [5].

The infrastructure of WMN is collected of fixed nodes interlinked via wireless links to form a multi-hop ad hoc network. Every node being either a router or a gateway acts as classical access point to mesh clients and/or connects to other nodes through point to point wireless links. Routers and gateways have a moderately established topology except for occasional failures or additions, while mesh clients may change their positions frequently. The wireless, WMNs and the risky security environment bring a great challenge to securing WMNs. Wireless communications are vulnerable to passive attacks such as eavesdropping, as well as to active attacks such as Denial of Service (DoS). Most schemes proposed recently are developed from security schemes of wireless local networks.

Revised Version Manuscript Received on August 11, 2016.

J. Srinivasan, Research Scholar, Department of Computer Science and Engineering, St. Peter's University, Chennai (Tamil Nadu)-600054. India.

S. Audithan, Professor, Department of Computer Science and Engineering, Ponnaiyah Ramajayam Institute of Science and Technology & University, Thanjavur, (Tamil Nadu)- 613403

The multi-hop routing in WMNs is a very vital and essential functionality of the network; and like all critical operations, an adversary may be tempted to attack it. The routing mechanism must thus be secured. Multi hopping has also an important effect on the network utilization and performance. In this paper, we introduce Anonymous Secure Routing Protocol ability to improve secure routing and reliability in multi hop WMNs. In ASRP we using onion routing to offers private communication over a public network. Onion routing is an infrastructure for private communication over a public network. Onion routing's anonymous connections are bidirectional, near real-time, and can be used anywhere a socket connection can be used. An onion is treated as the destination address by onion routers; as a result, it is used to establish an anonymous communication in the network.

The rest of this paper is prepared as follows. In section2, cover the related work. Section 3 we describe an Anonymous Secure Routing Protocol for Multi hops Wireless Mesh Network (ASRP). In Section 4, simulations and experimental evaluation discuss the packet transmission in ns-2 show the efficiency of our model. Section 5 presents the conclusion.

II. RELATED WORK

Safe Mesh [1] specifically consider hybrid WMNs to improve connectivity and reliability by exploiting communication resources available on client devices. It is extremely useful in emergency and disaster scenarios where a rapidly deployed mesh backbone might not provide sufficient coverage of the incident area and where first responders can be expected to be equipped with wireless mobile computing devices. This mechanism used to detect the availability of multiple links between neighboring nodes. The link selection mechanism also tries to ensure channel diversity and provide high throughput. However, this mechanism occur in link breakage thus result in partial route discovery and more costly.

Security architecture [2] ensures unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. This architecture strives to resolve the conflicts between the anonymity and traceability. It also includes guaranteeing fundamental security requirements for example confidentiality, authentication, non-repudiation, and data integrity. ID-based broadcast encryption scheme [3] to provide secure transmission keys for Mesh node in the trust domain, and ensure the confidentiality, non repudiation of the transmission. All Mesh nodes need to be authorized by the secure center, and receive the session keys from the Mesh Key Distributors (MKD) in those networks, since the service provider can conveniently account and manage users in networks. The mesh node in the trust domain can take advantage of transmission keys to transmit data with the multi-hops exchange information protocol, which greatly

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

improves the throughput and reduces the delay of data transmission in WMNs. Reliable WMN infrastructure with Quality of Service constraints [4] built reliable WMN that resists the failure of a mesh node and ensures full coverage to Mesh Clients. The proposed multi-objective optimization model is solved using meta-heuristics which provides the network operator with a set of reliable tradeoff solutions. This approach provides effectiveness, scalability, robust and cost-effective infrastructures. IEEE 802.11s WMNs [5] gives a detailed analysis of 802.11s framework. It provides a better understanding of the following questions for the emerging 802.11s standard: what performance can be expected from 802.11s WMNs, what problems still exist in 802.11s WMNs, and what direction can be taken to improve 802.11s mesh networking. Deflating link buffers in a WMNs [6] objective is to maintain high network utilization while providing low queuing delays. This mechanism improved on pre-set buffer allocations that cannot optimally work across the range of configurations achievable with 802.11 radios.

An anonymous on-demand routing protocol [7] ensures that adversaries cannot discover the real identities of local transmitters. It design based on broadcast with trapdoor information. This scheme prevents strong adversaries from tracing a packet flow back to its source or destination for location privacy.

The shared wireless medium [8] facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. A novel anonymous routing protocol can accomplish both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes under a rather strong adversary model. This protocol offers the anonymity of sources, destinations, and source-destination relationships in addition to node un locatability and intractability and end-to-end flow un traceability. It is also resistant to a wide range of attacks and preserves the high routing efficiency.

Anonymous Location-Aided Routing [9] designs a privacy-preserving and secure link-state based routing protocol. It uses nodes current locations to securely disseminate and construct topology snapshots and forward data. This scheme provides authentication, security, anonymity, privacy features, data integrity, and untraceability. It also offers protection against passive and active insider and outsider attacks. An unobservable secure routing (USOR) scheme [10] offers complete unlinkability and content unobservability for all types of packets. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers.

An Attack-Resilient Security Architecture (ARSA) [11] designed to be resilient to a wide range of attacks in WMNs. In this scheme proposed ticket-based anonymity scheme which resolution the conflicting security requirements of unconditional anonymity for truthful users and the traceable of misbehaving users. ARSA eliminates the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. ARSA supports efficient mutual authentication and key agreement both between a user and a serving WMN domain and between users served by the WMN domain.

III. PROPOSED SYSTEM

In this paper we propose Anonymous Secure Routing Protocol for Multi hop Wireless Mesh Network (ASRP) is a fixed infrastructure where the public and group key can be initially deployed in the mesh nodes. We design an onion encrypted secret message to verify the RREQ-RREP of nodes. Private key is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.

The Certificate Authority is issued private key and session key. In order to secure the secrecy while exchanging the route information, we design the packet formats of the RREQ and RREP, and modify the related processes. Onion Routing is a mechanism to provide private communications. In this mechanism, source node sets up the core of an onion with a specific route message. Every communication node adds an encrypted level to the RREQ message. The source and destination nodes do not necessarily know the ID of a communication node. The receiver node receives the onion and delivers it along the route back to the source.

Initially, the Sender node *S* broadcasts the RREQ packet to neighbor nodes in the network. If the receiver node *R* receives the RREQ, then it will reply the RREP packet back along the incoming path of the RREQ. The node *S* knows about *R*, it contain private key. *S* creates a new session key K_{SR} for the association among *S* and *R*. The following entry will be updated in *S*'s destination table.

The Sender S broadcast an RREQ packet format is given below.

$$R_{REQ}, H_{sn}, N_R, [N_{SR}, onion(S)]P_s \quad (1)$$

where R_{REQ} → packet type identifier

H_{sn} → Sequence number randomly generated by *S*

N_R → Encrypted message for the request validation at the receiver node

N_{SR} →Encrypted message for the route validation at the neighbor nodes

Onion(*S*) → key encrypted onion created by *S*

The whole R_{REQ} packet is finally signed by *S* with its private key P_s .The N_{SR} is a one-way function that creates by the S and sent to the R. The N_{SR} format is given below.

$$N_{SR} = S_k * Kv \quad (2)$$

where Kv →one-time nonce for the route discovery

S_k → symmetric key.

The secret message V_R is given below

$$V_R = (S_k * Kv) K_{SR}, P_R \quad (3)$$

If *R* is the receiver of the message, *R* can decrypt the second part of V_R through its private key P_R, and then decrypt the first part by the obtained K_{SR}. Now we describe the encrypted onion *Onion*(*S*). *S* creates the onion function as given below:

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

$$Onion(\mathrm{S}) = \mathrm{O}\,K_v * S_k \quad (4)$$

where K_v is a one-time nonce generated by *S*. The core is encrypted with the symmetric key of S_k, and can only be decrypted by *R* using symmetric key. The neighbor node *I* are receive the RREQ packet from the node *S*, these entries are stored in the routing table. The node *I* checks H_{sn} and timestamp in order to find whether the packet is expiry or valid. If the H_{sn} is not known in the routing table that RREQ is new otherwise that RREQ is expiry then removing this RREQ packet. Also the node *I* decrypts the V_R by its own private key. If the decryption is failure then the node *I* decide that RREQ is wrong and it comes from the malicious node so dropped this packet and report this node as malicious. If the RREQ packet is comes from real node the node *I* will design and broadcast another RREQ packet in the following format:

$$RREQ, N_{sq}, V_R, [V_{SR}, Onion(\mathrm{I})], \mathrm{P_I} \quad (5)$$

where $Onion(\mathrm{I})$ → the key-encrypted onion part is updated.

$\mathrm{P_I}$ → Group private key of node *I*

The node *I* updates the onion function in the following method

$$Onion(\mathrm{I}) = \mathrm{OS_{KI}}[\mathrm{N_I}, \mathrm{Onion(S)}]$$

where $\mathrm{N_I}$ →One-time nonce generated by *I*

Onion(*S*) is obtained from the received RREQ packet and the onion is encrypted with the symmetric key $\mathrm{S_{KI}}$ of node *I*. This process repeated until the receiver reaches the RREQ packet from the Sender.

While *I*'s RREQ reaches the next hop *J*, *J* executes the same actions and update the onion in the RREQ is given below

$$Onion(\mathrm{J}) = \mathrm{OS_{KJ}}[\mathrm{N_J}, \mathrm{Onion(I)}] \quad (6)$$

When the receiver node receives the RREQ from the neighbor nodes it can decrypts the part of V_R then it understands that it is the destination of the RREQ packet. R can obtain the session key $\mathrm{K_{SR}}$ and the validation key V_K. Then the R is prepared to send the RREP packet to the neighbor nodes. The RREP packet format is given below.

$$\mathrm{RREP}, [V_K, Onion(\mathrm{J})], \mathrm{K_{JR}} \quad (7)$$

where RREP is the packet type identifier, V_K and *Onion*(*J*) are obtained from the original RREQ and encrypted by the shared key $\mathrm{K_{JR}}$. The neighbor node J receives the RREP message from the destination then it decrypts the RREP packet.

$$[V_K, Onion(\mathrm{J})], \mathrm{K_{JR}} \quad (8)$$

If it successful decryption, the RREP is valid then it send the RREP packet to the next hop. The Sender node *S* receives the RREP packet, it will update the route table. Finish the route discovery process then the source transmits the data to the destination. The source transmit the data packet format is given below

$$\mathrm{DATA}, \langle P_{data} \rangle \mathrm{K_{SR}} \quad (9)$$

where *DATA* → packet type;

P_{data} →Data payload

$\mathrm{K_{SR}}$ →Session key

Upon receiving a data packet, every node checks the routing table. If the data packet matches the node will forward the packet to the anonymous next hop. Otherwise, the data packet will be discarded. This procedure is continuous until the data reaches the receiver node *R*. Finally the destination node receives the encrypted data and decrypts the original data by session key.

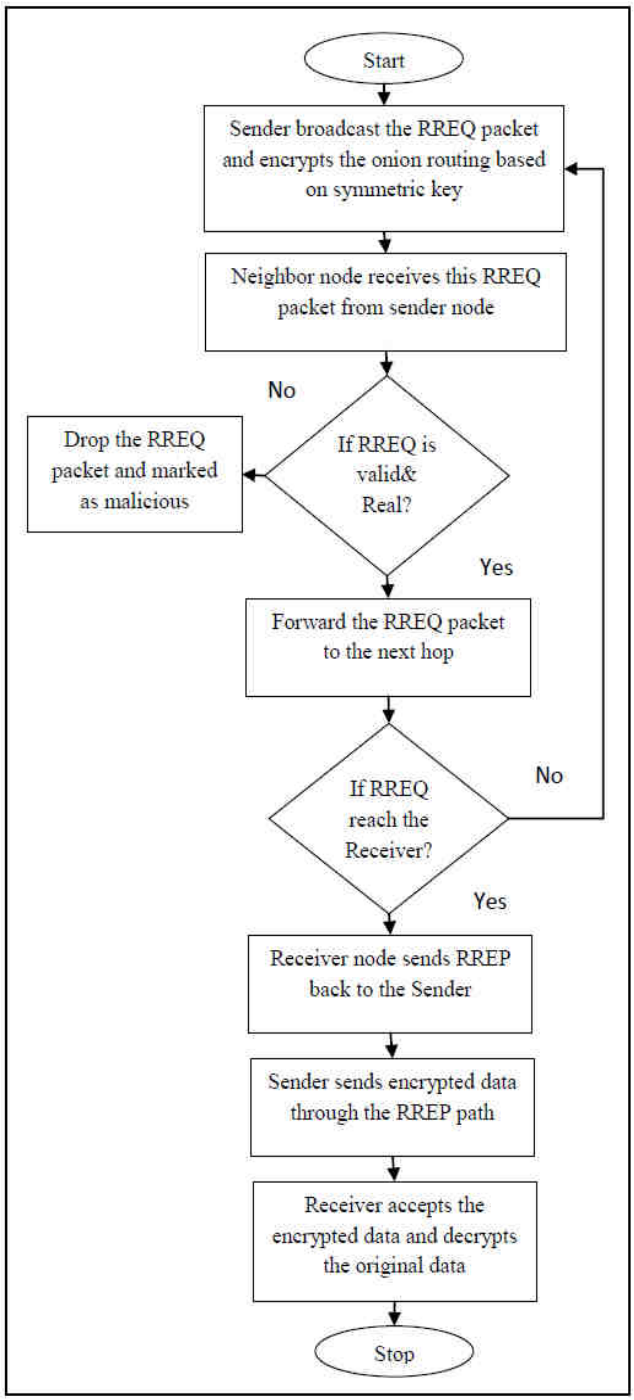

Figure 1: Flowchart of the ASRP Scheme

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

The figure 1 represents the flowchart of the proposed scheme. Initially the sender broadcast the RREQ packet to the neighbor nodes. The neighbor nodes are received the RREQ packet and check this packet is valid or expiry. If the packet is expiry dropped the packet. Then this packet is decrypt if the packet is wrong this RREQ send the node is malicious and notified to all nodes. Otherwise this RREQ packet is send to the next hop. The receiver node receives the RREQ packet then it send RREP packet back to the RREQ path. The Sender receives the RREP then it sends encrypted data to the RREP path. Finally the Sender accepts the encrypted data and it decrypts the original data.

IV. PERFORMANCE EVALUATION

In this section, we provide performance evaluation of the ASRP is analyzed by using the Network Simulator (NS2). This software is an open source programming language written in C++ and Object oriented Tool Command Language (OTCL). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The simulation of the ASRP scheme is described in table 1.

Table-1. Simulation parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	50 s
Number of nodes	50
MAC type	802.11
Traffic model	CBR
Antenna Model	Omni Antenna
Simulation Area	1000×1000
Transmission range	250m
Network Interface Type	Wireless PHY

In this proposed scheme, every node has the direct link with the nodes within the range 250m. The nodes are communicated with each other by using User Datagram Protocol (UDP). All the nodes receive the signal from all directions by using the omni-directional antenna. The performance of the ASRP scheme is analyzed by using the parameters Packet Delivery Rate (PDR), Packet Loss Rate (PLR), average delay, throughput and residual energy.

4.1. Packet Delivery Rate

The Packet Delivery Rate (PDR) is the rate of number of packets delivered to all destinations to the number of data packets sent by the source node. PDR is measured by the equation 10.

$$PDR = \frac{\sum_0^n Packets\ Received}{Time} \qquad (10)$$

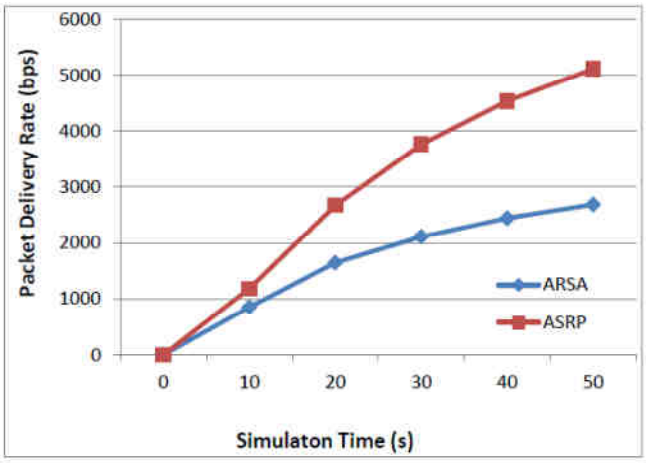

Figure2: PDR of ASRP and ARSA

The figure 2 refers the PDR of the proposed scheme ASRP is higher than the PDR of the existing method ARSA.

4.2. Packet Loss Rate

The Packet Loss Rate (PLR) is defined as the difference between the sent packets and received packets in the network per unit time as in equation 11.

$$PLR = \frac{\sum_0^n Sent\ Pkts - Rcvd\ Pkts}{Time} \qquad (11)$$

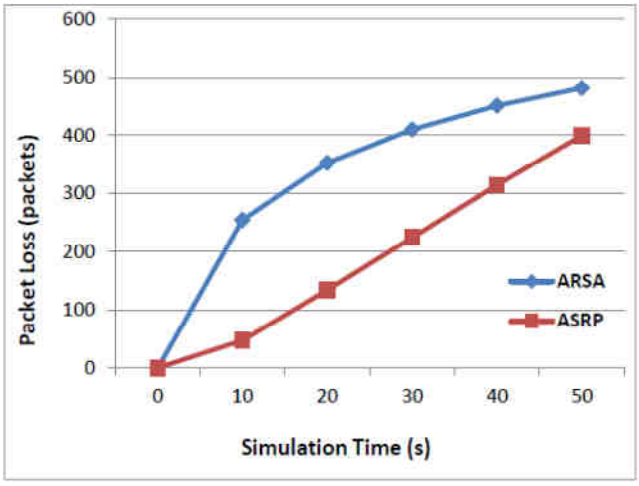

Figure 3: PLR of ASRP and ARSA

Figure 3 indicates that the total packets lost of ARSA are greater when compared to the ARSA mechanism. The ASRP has reduced packets lost due to highest security routing.

4.3. Throughput

Throughput refers to the total number of packets successfully delivered across the network for every 1000 packets sent. Throughput is obtained using equation 12.

$$Throughput = \frac{\sum_0^n Packets\ Received(n) * Packet\ size}{1000} \qquad (12)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

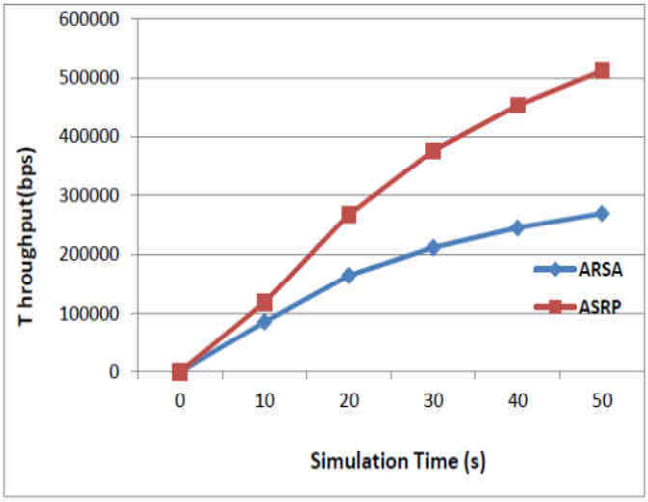

Figure 4: Throughput of ARSA and ASRP

Figure 4 show that ASRP has greater average throughput when compared to the ARSA mechanism. The security activity has improved the network performance greatly.

4.4. Average Delay

The average delay is defined as the time difference between the current packets received and previous packets received. It is measured by the equation 13. Where n is the number of nodes.

$$Avg\_Delay = \frac{\sum_{0}^{n}(Packet\ Received\ Time - Packet\ Sent\ Time)}{n} \quad (13)$$

The average delay value is plotted in figure 5, which shows that the delay value is low for the proposed scheme ASRP than the existing scheme ARSA. The minimum value of delay means that higher value of the throughput of the network.

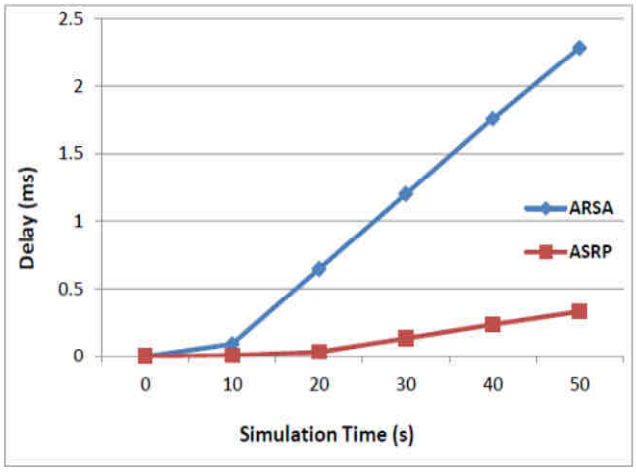

Figure 5: Delay of ASRP and ARSA

V. CONCLUSION

WMNs have become an essential focus area of examine in the recent years due to their great application in realizing numerous next-generation wireless services with Quality of Service guarantees and with high connectivity support for the users. It increasing demand for rich, high-speed and bandwidth intensive content access, recent research has focused on developing high performance communication and security in the network. In this paper we have analyzed the Anonymous Secure Routing Protocol for Multi hop Wireless Mesh Network (ASRP) to achieve desired security objectives. The key-encrypted onion routing is designed to prevent intermediate nodes from inferring a real receiver node. Simulation results indicate that increase the throughput and reduce the packet loss to the efficiency of the proposed ASRP protocol.

REFERENCES

1. Asad Amir Pirzada a, Marius Portmanna,b, Ryan Wishart a, Jadwiga Indulska, SafeMesh: A wireless mesh network routing protocol for incident area communications, Pervasive and Mobile Computing, vol.5, pp.201-221, 2009.
2. J. Sun, C. Zhang ; Y. Fang, A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks, IEEE 27th Conference on Computer Communications, 2008.
3. Yahui Li, Xining Cui, Linping Hu, Yulong Shen, Efficient Security Transmission Protocol with Identity-based Encryption in Wireless Mesh Networks,IEEE, 2010.
4. D. Benyamina A. Hafid, M. Gendreau b, J.C. Maureira, "On the design of reliable wireless mesh network infrastructure with QoS constraints", Computer Network, vol.55, pp. 1631-1647, 2011.
5. Jaydip Sen, "Security and Privacy Issues in Wireless Mesh Networks: A Survey", Innovation Labs, Tata Consultancy Services Ltd. Kolkata, INDIA.
6. Kamran Jamshaid Basem Shihada Ahmad Showail, Philip Levis, Deflating link buffers in a wireless mesh network, Ad Hoc Networks 16 (2014) 266–280.
7. J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.
8. MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks Yanchao Zhang, Student Member, IEEE, Wei Liu, Wenjing Lou, Member, IEEE, and Yuguang Fang, Senior Member, IEEE.
9. K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Trans. on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.
10. Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," IEEE Trans. on Wireless Communication, vol. 11, no. 5, pp. 1922–1932, May. 2012.
11. Yanchao Zhang, and Yuguang Fang, ARSA: An Attack-Resilient Security Architecture for Multi hop Wireless Mesh Networks, IEEE Journal On Selected Areas in Communications, Vol. 24, no. 10, 2006.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.