International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Secure Routing Algorithm in Wireless Mesh Network

Rajnikant Narwade, P. Balamurugan

Abstract— In the today's' era of communication technology disaster management plays important role in life saving. Regardless of men made disasters or natural disasters proper communication network can be used to exchange information. In natural calamities wireless sensor mesh network proved to be as good option for communication. Low-altitude Unmanned Aerial Vehicles (UAVs) which is associated with WLAN Mesh Networks (WMNs) can be used in disaster management areas. The advantage of it is it can be installed on demand and it can use for efficient exploration of sized areas. The WMN is consisting of different components such as mesh clients, mesh routers and base station. It is more prone to have attacks of different types such as Denial of Service attack, black hole, gray hole , reply attack, Sybil attack etc. The most important attack which can damage whole working of WMN is routing attack. IEEE 802.11i is used as standard protocol for security in WLAN and IEEE 802.11s is used as secure algorithm for communication in WLAN mesh network. But both of them fail to address issue of routing problem in WLAN mesh network. The primary purpose of this paper is to outline routing algorithm and to design assured routing protocol. In this paper we have proposed improved secure Position-Aware, Secure, and Efficient mesh Routing approach (S-PASER). The proposed mechanisms have obviated more attack than regular IEEE 802.11s/i security mechanism and well known, secure routing protocol. The proposed methodology can be implemented on omnet++ simulator. The simulation results proved to be have better performance and throughput than existing algorithm.

Keywords— Secure routing protocol, Wireless sensor network, mesh network, IEEE 802.11s, IEEE 802.11i, PASER, routing attacks.

I. INTRODUCTION

"**Disaster management**" signifies comparable to and associated procedure of arranging, sorting out, planning and actualizing those necessary estimates which are noteworthy or delightful for avoidance of peril or danger of any calamity, alleviation or decrease of danger of any fiasco or its seriousness or radiation, limit building, status which manage the any catastrophe, brief reaction to any undermining debacle circumstance or calamity, surveying the seriousness or greatness of impacts of any calamity, clearing, salvage and help, restoration and remaking [1].

Manuscript received on April 02, 2020.
Revised Manuscript received on April 20, 2020.
Manuscript published on May 30, 2020.

* Correspondence Author
Mr. Rajnikant Kundlik Narwade*, Research Scholar, Department of Computer Science and Engineering, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.
Dr. P. Balamurugan Professor, Department of Computer Science and Engineering, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.

Calamity can be partitioned into basically two sort's artificial debacles and cataclysmic events.
The most influenced disasters can be listed are earthquakes, Hurricanes and tropical storms, landslides & debris flow, tsunamis, winter and ice storms, terrorist attacks, wars etc. In the earthquake of 2010 which is occurred in Haiti alone which claimed 230,000 people's lives [3]. When the disaster occurs, the destroyed areas are in turmoil. It destroys communication system, transport system and merely disunite from helping areas. In such critical areas it is very difficult to set network and build communication network system. With minimum resources like sensors, base station and cluster heads wireless ad-hoc system can be set. As wireless sensor networks contains minimum resources for setting communication network.

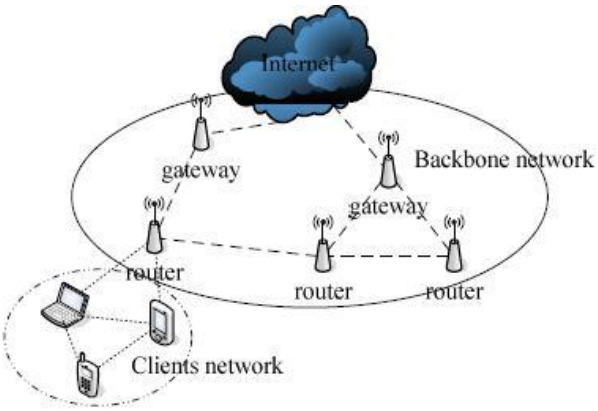

Figure 1: Practical Example of a WMN [4]

Wireless mesh networks can be attainable with the different remote innovation which incorporates 802.11, 802.15, 802.16, cell advances or blends of more than one sort.
Wireless mesh network, which utilizes packet switched network including a static wireless backbone [5] [6]. It depends on two sorts of routing protocols utilized in wireless mesh network i) topology based routing protocol and ii) position based protocols.

Topology based routing protocols: It utilizes topological data to pick way between hubs. It is divided into two categories a) proactive protocol: it uses periodic updates of routes to maintain routes between nodes b) reactive protocol which is also called as "on-demand", paths will be calculated whenever required.
ii) Position based protocol it uses geographical information to set path between nodes
General gathering of various applications utilized in WMNs are recorded beneath [7]:

- Broadband home network
- Enterprise networking
- Metropolitan area network
- Automation of Building
- Transportation System
- Health and Medical science
- Security and the surveillance
- Warehouse
- Disasters reporting & emergency networking.

Because of the functionalities gave by WMN's having the reliable and quicker wireless connectivity, so it is used in various territories, for example, clinics, lodgings, eateries, air terminal lounges and in a lot more places where the huge groups consistently assembles.

Routing Layer Challenges

Many routing protocols exists for wireless mesh network, still routing is prominent area of research in wireless mesh network [8].

Multiple Performance Metrics: Most of routing protocols uses hop count, time, geographical distance to analyse performance of routing protocol. The performance metric should be based on network and application. Random metric selection of performance can lead to false prediction of routing protocol performance.

Scalability: It is one of big challenge of routing protocol. As wireless mesh network are built in disaster, initially the size of network is unknown. It is critical to have a scalable routing protocol in WMNs, as the wireless network is very large which may takes a long time to set up or maintain a routing path.

Robustness: Regardless of several disturbances routing in WMN is expected to remain robust. It should address problems like congestion, link failure, load balancing, route discovery etc.

Efficient Routing with Mesh Infrastructure: WMN is composed with mesh clients, mesh routers. Mesh clients have low power batteries. Routing should have efficiency over low power mesh clients and routers. It should not consume much power for updating routing table.

Attacks on routing

The WMN is vulnerable with different types of attacks. The large impact attacks are listed below:

Passive attack

A passive attack does not disturb the normal functioning of wireless mesh network. It only steals the data and tries to get benefit from gained information. The communicating parties does not know that network is get attacked by attackers. Traffic analysis, eavesdropping are example of passive attack. A strong encryption algorithm can prevent wireless mesh network from passive attack.

Active Attack

In active attack the communicating parties knows that network is attacked. In active attack attacker disturbs communication, can damage communication links and can make further changes in network. It confuses routing procedures and degrades network performance.

Diversion of Route

A malicious node can originate diversion attack on route by manipulating the mutable fields such as number of hops, source & destination and header elements, etc. To divert the route, it can also announce itself as source and other node as destination, due to which the packet is misrouted. In this fashion network traffic can be routed at any node by malicious node, it can generate reverse path also to increase congestion which can lead to degradation of network performance.

Routing Loops

By spoofing MAC addresses and controlling the adjustments in the estimation of the measurement field, may prompts make routing loops in a wireless mesh network. Rest of the segment of the paper is clarified as follows. We talk about the related work in Section II and feature of PASER with included worth highlights. A short time later we are examining on the structure squares of PASER in Section III. We think about security highlights of PASER and its options utilized regarding the requirements of secure routing in UAV-WMN are introduced in Section IV. Broad execution assessment of every single imaginable arrangement is examined in Section V. In the Section VI, paper end with outline of the outcomes.

II. RELATED WORK

Dajun Chen, Chao Wang proposed an Ant-Based Trusted Routing Algorithm for wireless mesh network [9]. This system doesn't instate the routing table; it expects the uniform conveyance of parcels at every goal. Earlier information on topology is required to refresh the routing table. At the point when the neighbour hub is considered as the goal hub, the estimation of the default introduction likelihood is huge to the point that the source hub can arrive at the goal hub just by a connecting, which spares the system assets. Ant colony algorithm works in corresponding with positive criticism technique which ends up being an extremely productive protocol for communication. This algorithm is utilized to locate an exact route with generally brief timeframe with diminished start to finish delay. This algorithm is tried on omnet++ simulator. By considering parameter, for example, start to finish delay, pace of packet delivery and overhead in routing; this demonstrated it is to be better than ATR, AODV and DSR calculation.

In [10] and [11], Srinivasan has determined the optimal throughput for each node through assumption that forwarding actions are performed by selfish interest. Research proposed GTFT (Generous Tit For Tat) algorithm where centralized mechanism is used to control distributed nodes. In [12], proposed mechanism has proved maximum throughput by having approach of forwarding data as received from previous nodes. As the Routing protocols achieve Pareto optimality, the proof of cheat and absolute fairness is to be suggested. SPRITE [13] which characterizes it is an imaginative procedure which authorizes sending is the best system. Anderegg et al. Structured Ad Hoc-VCG [14], a routing protocol based on notable Vickrey, Clarke, and Groves sell off, which is utilized to ensure that each transitional hub are discounted in any event the expense caused to transfer the packets, and it needs to carries on as indicated by the given protocol particulars. The Commit conspire [15] further built up this way to deal with fortify the honesty property, in any event, when the source hub carries on deliberately.

Liu [16] characterized another confirmation protocol/proposed new calculation, permits neighbouring hubs to validate themselves without uncovering their unique personalities. The goal addresses are utilized for route revelation; we accomplish the contingent secrecies for goal. The creators concentrating on the traffic protective measures by proposing a punishment based routing algorithm in [17]. Be that as it may, they have done the utilization of source routing plan for their protocol and additionally they overlooked to manage character protection without referencing how verification is done between mesh hubs. The creators of [18], [19] introduced a verification scheme utilized for WMNs, which is flexible against mesh routers trade off and a portion of the other general protection mindful confirmation methods are depicted in [20], [21]. A protected multi-path Hybrid routing protocols, MHRP, is proposed in the [22]. We have not considered Privacy-safeguarding of the end-clients right now. Ashish Nanda, Priyadarshani Nanda have presented a Secure geo location oriented routing protocol which is utilized for wireless mesh network [23]. This algorithm specifies the multilevel security mechanism by specifying encryption and decryption methodology. It is treated as the hybrid routing protocol which is designed in the support of large, sense and dynamic networks without compromising the reliability and security produced by the network and the devices used in it[24]. This algorithm is designed to be used in the high performance devices such as smart phones, tablets, laptops, etc., but also keep in mind that it must be having the highest performance power and which uses the Symmetric and asymmetric encryption and decryption algorithms. N. Ben Salem proposed mechanism in which work is emphasized on identifying the weak factors of WMN where it will require more attention and suggested a more secure operation. The method does not consider the class set of attack on mesh clients and malicious node behaviour. Capkun have developed a mechanism where privacy of communication node is going to be preserved in a hybrid ad-hoc network, which is similar to wireless mesh network [25]. The anonymity and privacy preserving characteristics for mobile nodes are provided by this methodology. Zhang developed attack resilience system architecture for multi-hop wireless network. The technique is moulded with wireless mesh network as e-commerce based on credit card. Zhang proposed an identity-based cryptosystem for authentication and key agreement between mesh clients and routers. SAODV-Secure Ad hoc On Demand Distance Vector is a proposed augmentation of secure AODV Routing packet, by utilizing digital signature and hash chain strategy, it can keep up the security protocol. Digital signature is utilized to confirm the non-discretionary fields of the message and hash fasten is utilized to keep up security of hop count data. As SAODV utilizes asymmetric cryptography, it requires a key management mechanism. A hub can ready to sends a route demand and a route answer by setting up of Max_Hop_Count field to the TimeToLive (TTL) field from the IP header, set a hash field to arbitrary seed value, which figures out Top Hash by hashing irregular seed for Max_Hop_Count times. A hub gets a route demand or a route answer message; at that point it applies the hash function Max_Hop_Count minus Hop Count times to the incentive in the Hash field, and afterward the outcome esteem is contrasted and the worth contained in the Top Hash field to create the outcome. In the event that the intermediate hubs can answer to a route demand for the benefit of the last goal, the expansion of the signature is utilized to answer to the route journey. In any case the route solicitation will be sent by the intermediate hubs.

The proactive secure link state routing solution for an ad-hoc system is given by Secure Link-State Protocol (SLSP) [28]. In a proactive routing protocol, every hub in the system keeps up at least one routing tables which are refreshed without fail. For the most part every hub sends a communicate message to a whole system to check any progressions happen in the system. Additional overhead will be added while updating routing table and up-to-date result information in the protocol. SLSP hubs communicate their connection updates to keep up topological data for a subset of system hubs with R hops. Hub's public key endorsements are communicated inside their zone with the assistance of signed public key distribution (PKD) packets. Link state data is communicated after certain time interim by utilizing Neighbour Location Protocol (NLP). While accepting a Link state update (LSU) packets, each hub check the attached signature utilizing a public key, which they recently trapped in the pubic key distribution period of the protocol to validate the hop count by one way hash chains. To distinguish change among IP and MAC addresses tends to utilizing Neighbour revelation procedure and NLP, SLSP offers security against individual malevolent hubs. However, SLSP is hazardous which to intriguing assailants that create non-existing connections between themselves and flood this data with their neighbouring hubs.

Kimaya Sanzgiri [29] proposed another security protocol named as Authenticated Routing for Ad-hoc Networks (ARAN). The ARAN algorithm depends on AODV independent protocol; which utilizes public key certificates signed by a confided authority. This algorithm is related with its IP address utilizing an public key so as to accomplish the security objectives of confirmation and non-renouncement. Right now public key cryptography is utilized, where the taking an interest parties realizes the public key which is to be utilized for the verification reason. ARAB algorithm utilizes cryptographic certificates which permit confirmation, message-respectability and non-disavowal to route discovery packet (RDP). This incorporates a packet type identifier, goal IP address, source hub's private key. Switch way is a lot of hub subsequent to accepting the RDP message. Approval is finished by the collector to approve the signature utilizing public key and declarations of the ancestor. The sink hub checks substance of the message, includes certificate, and forward communicates the message to each neighbour hub. The signature of beneficiary hub is utilized to keep noxious hubs from embeddings self-assertive route discovery packet that changes routes or form loops. To acquire turn around way the RDP message is utilized. It gives a packet type identifier, IP address of source and IP address of goal.

Every hub refreshes the data utilizing RDP packet alongside the converse way. At whatever point the protocol utilizes cryptographic certificate; the correspondence ensures the start to finish confirmation in the middle of the hubs. ARAN algorithm is a basic protocol, which won't require any extra overhead. The overhead of the protocol increments, when the quantity of hubs expanded in the network.

III. PROPOSED METHODOLOGY

Secure PASER procedure is a proficient, solid, secure route discovery protocol utilized for wireless mesh network. This system gives a route to a hub wishing to send a packet to a goal hub. Thus, PASER affirms that the route which is found is having the exactness regarding metric and legitimized hubs when there is a nearness of outside assailants. In addition, it guarantees that negligible assets expended in the system. That is, the PASER expects to guarantee the dependability of the system and the accessibility of its administrations in an effective way.

The routing of the information in exceptionally unique WMNs is a basic structure hinder that unequivocally impacts the exhibition and unwavering quality of the wireless network. Because of the versatility of the hubs and because of radio propagation dynamics (e.g., blurring), the exceptionally unique WMNs have quickly changing connectivity.

As the consequence of mechanism, hub sets are consistently associated and organize interfaces frequently breaks.

The PASER mechanism expects the accompanying network model and attacker model.

Network Model: Wireless mesh network consist of mobile (UAV) nodes and static node which works as a ground station as a Centralized system which coordinates the network with a single organization is assumed to access the network. Legitimate operator sticks to protocol, but malicious nodes might be deviating protocol from them. It uses public key infrastructure in which a network operator acts as a certification authorities. Real hubs have certificates with incorporated jobs (gateway, access point or router). The network operator must run a protected Key Distribution Center (KDC) which is dependable to powerfully deal with all the system accreditations. All the hubs know the public key of the KDC. This permits whenever; mesh gateways can set up a dependable association with the KDC and the other way around. In UAV-WMN, this can be acknowledged by running the KDC at the ground station. It is expected that the genuine hubs incorporates the positioning device that runs a secure navigation service, for example, the Galileo Public Regulated Service [30]. That is, the objective situation is thought to be outside and to have low obstructions, as in UAV-WMN.

Attacker Model: As the assailants makes an assault which upset correspondence framework and assaults on security of routing. The attacker is expected to control all the outside hubs which will have more force with preferred correspondence vitality over the real hubs. The attacker likewise bargains with real hubs or system certifications, by methods for social building, physical assaults, cryptanalysis, and others. The attacker itself can go about as a real hub by securing all conceivable data of real hub. The attacker model should work in the field of bogus routing, dropping of packet, keep up delay in correspondence and so forth to recoup the loss of data and the system.

IV. PERFORMANCE ANALYSIS

The secure PASER is implemented in Linux platform using OMNET++ [31] simulator by keeping following objectives in mind or it can be developed by using Mat lab also.

1) Node registration
2) Detection of various routing attacks
3) Minimizing the packet drops
4) Increasing the throughput of wireless mesh network.

As links of WMN are very dynamic and asymmetric, best efforts will be needed for a route discovery and route maintenance. The performance of secure PASER algorithm is decided to use following routing metrics:

1. Hop Count

Hop Count is the essential component which is utilized to figure out the exhibition of the routing algorithm. For the most part the basic routing protocols, for example, AODV, DSR, DSDV, and so on. Which are intended for multi-hop wireless network systems with the utilization of hop count as metric. It discovers paths which have the most shortest number of hops. In the situations of high portability, hop count which can beat the other burden dependent metrics. This is for the most part the after effect of a metric's dexterity. It is additionally a metrics with high stability which further has the isotonic property, to permits least weight paths to be found effectively.

2 Expected Transmission Count (ETX)

We characterize the Expected Transmission count (ETX) is the quantity of transmissions which are required to effectively convey a packet over the remote connections. The ETX of a path comprises of the entirety of ETX of each connection alongside the path.

The ETX is estimated in connection of a genuine system by

$$ETX = 1/(Df * Dr)$$

Where Df represents the forward conveyance proportion ratio, and Dr for the opposite conveyance proportion ratio. The conveyance proportions Df and Dr both are estimated by communicating devoted connection probe packets with a fixed size of each normal period (a typical value is 1 second) from every one of the hub to its neighbour hubs.

3 Expected Transmission Time (ETT)

The Expected transmission time (ETT) metric is characterized as an augmentation of ETX, which may considers packet size and the connection transfer speed (bandwidth). ETT is relied upon time to be effectively transmit a packet at the given MAC layer and it is characterized for a solitary connection as follows

$$ETT = ETX *S/B$$

Where, S means the average size of packet and B signifies current connection data transfer capacity. ETT path metric is acquired by including the entirety of the ETT estimations of the individual connections in the got path.

V. EXPECTEFD OUTCOMES

The Wireless Mesh Network (WMN) is a dynamic network where it contains the mesh nodes, mesh routers etc. It is expected to achieve diversion routing attack detection accuracy more than 90 percent and the throughput of the network, which is to be dependent on the number of packets transmitted by the sender node and number of packets received by the receiver node is expected to be more than 92 percentages.

VI. CONCLUSION

A Wireless mesh network is characterized as a dynamic network consisting of the mesh nodes; mesh routers which are connected to base station. The wireless mesh network is highly successful in communication in disaster management, where the normal network cannot be set easily. As it can be installed in men made disasters like terrorist attacks or research areas like volcano analysis, the communication data is very important. As wireless mesh network is set in disaster area no more secure equipment's are installed with it. A secure routing algorithm with an asymmetric cryptographic algorithm proves to be a better solution for routing attacks.

Database

Acronym	Definition
UAV	Unmanned Aerial Vehicle
WMN	WLAN Mesh Networks
PASER	Position-Aware, Secure, Efficient mesh Routing Approach
AODV	Ad Hoc On-Demand Distance Vector
DSR	Dynamic Source Routing
ATR	Augmented Tree-based Routing
GTFT	Generous Tit For Tat
SPRITE	simple, cheat-proof, credit-based system
VCG	Vickrey, Clarke, and Groves
GLOR	Geo-Location Oriented Routing
SAODV	Secure Ad hoc On Demand Distance Vector
SLSP	Secure Link-State Protocol

Table no 1: Acronyms Database

REFERENCES

1. www.mrsac.gov.in/projects/software-development-project/dmis
2. M. Sbeiti, N. Goddemeier, D. Behnke, and C. Wietfeld, "Paser: Secure and efficient routing approach for airborne mesh networks," IEEE Transactions on Wireless Communications, vol. 15, no. 3, pp. 1950– 1964, 2016.
3. J.-S.Huang, Y.-N.Lien, "Challenges of emergency commumcation network for disaster response", Communication Systems (ICCS) 2012 IEEE International Conference on. IEEE, pp. 528-532, 2012. Na Wang, Hengjun Wang, "A Security Architecture for Wireless Mesh
4. Network," cesce, vol. 2, pp. 263–266, 2010 International Conference on Challenges in Environmental Science and Computer Engineering, 2010.
5. S. Waharte, R. Boutaba, J. Iraqi, and B. Ishibashi, "Routing Protocols in Wireless Mesh Networks: Challenges and Design Considerations", Multimedia Tools and Applications Journal, vol. 29, no. 6, 2006
6. A. Zakrzewska, L. Koszalka, I. Koszalka, A. Kasprzak, "Analysis of Routing Protocol Performance in Wireless Mesh Networks", International Conference on Computational Science and Its Applications (ICCSA), pp. 307-310, June 2010.
7. S.Y. Shahdad, A. Sabahath, R. Parveez, "Architecture issues and challenges of wireless mesh network", International Conference on Communication and Signal Processing (ICCSP 2016), pp. 0557-0560, 2016.
8. Pavan Kumar Ponnapalli. "Wireless Mesh Networks: Routing Protocols and Challenges", Communications in Computer and Information Science, 2010
9. Dajun Chen ; Chao Wang ; Qiang Lin, "Ant-Based Trusted Routing Algorithm for Wireless Mesh Networks", 2009 Asia Pacific Conference on Postgraduate Research in Microelectronics & Electronics (Prime Asia)
10. V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao,
11. "Cooperation in wireless ad hoc networks," in Proc. IEEE INFOCOM, 2003, vol. 2, pp. 808–817.
12. V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "An analytical approach to the study of cooperation in wireless ad hoc networks," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 722–733, Mar. 2005.
13. W. Yu and K. J. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," IEEE
14. Trans. Mobile Comput., vol. 6, no. 5, pp. 507–521, May 2007.
15. S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE INFOCOM, 2003, pp. 1987–1997.
16. L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in Proc. ACM MobiCom, 2003, pp. 245–259.
17. S. Eidenbenz, G. Resta, and P. Santi, "The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," IEEE Trans. Mobile Comput., vol. 7, no. 1, pp. 19–33, Jan.2008 Y. Zhang, W.Liu and W.Luo, "Anonymous Communication in Mobile Ad Hoc Networks," in proceedings of INFOCOM, 2005.
18. W. Taojun, X. Yuan and Y.Cui, "Preserving traffic privacy in Wireless Mesh Networks," in proc of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06).
19. X. Lin, R. Lu, P.-H. Ho, X. Shen, and Z. Cao, "Tua: A Novel
20. Compromise- Resilient Authentication Architecture for Wireless Mesh
21. Networks," IEEE Wireless Communication, vol. 7, no. 4, pp. 1389-1399, Apr. 2008.
22. X. Lin, X. Ling, H. Zhu, P.-H. Ho, and X. Shen, "A Novel Localized
23. Authentication Scheme in ieee 802.11 Based Wireless Mesh
24. Networks," Int'l J. Security and Networks, vol. 3, no. 2, pp. 122-132, 2008.
25. K. Ren, W. Lou, K. Kim, and R. Deng, "A Novel Privacy Preserving
26. Authentication and Access Control Scheme for Pervasive Computing
27. Environment" IEEE Trans. Vehicular Technology,vol. 55, no. 4, pp.
28. 1373-1384, July 2006.
29. K. Ren and W. Lou, "Privacy-Enhanced, Attack-Resilient Access Control in Pervasive Computing Environments with Optional Context
30. Authentication Capability," ACM Mobile Networks and Applications
31. (MONET) (special issue on wireless broadband access), vol. 12, pp. 79-92, 2007.
32. Y. Zhang and K. Ren, "On Address Privacy in Mobile Ad Hoc Networks," ACM/Springer Mobile Networks and Applications
33. (MONET), vol. 14, no. 2, pp. 188-197, Apr. 2009.
34. M. Siddiqui, et.al, "MHRP: A Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network", IEEE MILCOM, Oct. 2007.
35. Ashish Nanda ; Priyadarsi Nanda," Secure-GLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks", 2017 IEEE Trustcom/BigDataSE/ICESS
36. A. Nanda, P. Nanda, and X. He. "Geo-Location Oriented Routing Protocol for Smart Dynamic Mesh Network." In High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on, pp. 891-898. IEEE, 2016
37. N. Ben Salem and J.P. Hubaux, "Securing Wireless Mesh Networks,"
38. IEEE Wireless Communication, vol. 13, no. 2, pp. 50-55, Apr. 2006.
39. S. Capkun, J. Hubaux, and M. Jakobsson, "Secure and privacy preserving communication in hybrid ad hoc networks," Swiss Fed. Inst. Technology.,-DIICA, Lausanne, Switzerland, 2004.
40. Y. Zhang and Y. Fang, "ARSA: An attack resilient security architecture for multihop wireless mesh networks," IEEE Journal on Selected Areas in Communication, Vol.24 No.10, October,2006.
41. P. Papadimitratos, and Z.J. Haas, "Secure Link State Routing for Mobile Ad hoc Networks," Proc. IEEE Workshop on Security and
42. Assurance in Ad hoc Networks, IEEE Press, 2003, pp. 27-31.

43. Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer, "Authenticated Routing for Ad Hoc Networks", Proceedings of IEEE journal on selected areas in communications, Volume 23, No. 3, March 2005
44. (2014) The Galileo Public Regulated Service - PRS. European GNSS Agency. [Online]. Available: http://www.gsa.europa.eu/security/prs
45. H. R. Shaukat, F. Hashim, "MWSN Modeling Using OMNET++ Simulator", *2014 5th International Conference on Intelligent Systems*, pp. 597-602, 2014.

AUTHOR PROFILE

Mr. Rajnikant Kundlik Narwade, obtained bachelors in Information Technology from Dr. BAMU University, Aurangabad. He has also obtains masters in Computer Science from JNTU, Hyderabad. Telangana. Currently he is working as research scholer in the department of Computer Science and Engineering,VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University) Avadi, Chennai, Tamilnadu, India.

Dr. P. Balamurugan obtained B.E. in Computer Science and Engineering from Madurai Kamaraj University in 2003 and M.E. in Computer Science and Engineering from Manonmaniam Sundaranar University in 2006. He has awarded PhD in Wireless Sensor Network from Anna University, Chennai in 2013. He is currently working as a Professor in Department of Computer Science and Engineering at VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology (Deemed to be University), Chennai, Tamil Nadu, India.