www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16340-16346

Review on Secure Routing in Wireless Adhoc Networks

Ugendhar Addagatla[1], Dr. V. Janaki[2]

[1]Department of C.S.E, Guru Nanak Institutions Technical Campus,
Ranga Reddy, Telangana-501506
ugendhar2008@gmail.com

[2]Department of C.S.E, Vaagdevi Engineering College,
Warangal, Telangana-506005
janakicse@yahoo.com

Abstract: ***Adhoc network, because of dynamic behavior, self sustaining approach, and non-reliability of infrastructure has made this network a major communication approach for future usage. These networks are benefited by adaptive node integration and dynamic routing for data exchange. Adaptive routings has high significance of data exchange, with adaptive network performances such as high throughput, low power dissipation, less interference, and long lasting networks. However with the advantage of having dynamic routing behavior in adhoc network, optimal routing and its selection remains an open issue to solve. To achieve the objective of optimal routing based on node characteristic and network property, various methods were developed in past. This paper, outlines the methods developed towards secure routing for robust and reliable routing in wireless adhoc network.***

Keyword: Secure routing, Wireless adhoc network, Node characteristic, robust routing.

1. Introduction

Recent advances in wireless technology have equipped portable computers, such as notebook computers and personal digital assistants with wireless interfaces that allow networked communication even while a user is mobile. A particular kind of wireless network called mobile ad hoc networks is presently under development. A mobile ad hoc network is a self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The network nodes communicate with one another over scarce wireless channels in a multi-hop fashion. The ad hoc network is adaptable to the highly dynamic topology resulted from the mobility of network nodes and the changing propagation conditions. These networks are used in emergency disaster rescue operation, tactical military communication and law enforcement. In these applications, where a fixed backbone is not available, a readily deployable wireless network is needed. Mobile ad hoc networks are also a good alternative in rural areas or third world countries where basic communication infrastructure is not well established. Another interesting application of mobile ad hoc networks is ubiquitous computing. Intelligent devices are connected with one another via wireless links and are self-organized in such a way that a newly joined node can request service from local servers without any human intervention. With the development of the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Some examples of possible uses include students using laptops to participate in an interactive lecture, business associates sharing information during a meeting, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Because of the mobility of the nodes, the network topology may change rapidly and unpredictably. Due to mobility constraint of nodes the network operational characteristic is unpredictable. Hence a route selected would not be optimal after a communication period. To develop a routing scheme most reliable in adhoc network, secure routing are need. The approaches of secure routing in adhoc network is reviewed as outlined in following section.

2. Secure Routing – Past Approaches

The limited resources in MANETs have made designing of an efficient and reliable routing strategy a very challenging problem. An intelligent routing strategy is required to efficiently use the limited resources while at the same time being adaptable to the changing network conditions such as: network size, traffic density and network partitioning. In parallel with this, the routing protocol may need to provide different levels of QoS to different types of applications and users. Nodes in MANETs often have limited energy supplies. Thus, to increase the network lifetime, a node should optimize its energy usage. In the communication system, the wireless interface between two nodes is the largest consumption of energy. The wireless interface consumes energy not only during active communication but also during passive listening, when it is idle. Studies show that energy consumption while listening to data is only slightly less than it is while actually receiving data. Thus, in the case of moderate traffic load, idle time is the dominating factor in energy consumption. The other major factor in Ad Hoc management is the node mislead. Although an efficient power management scheme is applied to a ad hoc network to a misleading node may result in the

improper routing of packet which may extend to the complete collapsing of the network also. In mobile ad-hoc networks, where nodes act as both routers and terminals, the nodes have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes. Mislead means aberration from normal routing and forwarding behavior. It arises for several reasons. When a node is faulty, its erratic behavior can deviate from the protocol and thus produce non-intentional mislead. Intentional mislead aims at providing an advantage for the misleading node. An example for an advantage gained by mislead is power saved when a selfish node does not forward packets for other nodes. An advantage for a malicious node arises when mislead enables it to mount an attack. Without appropriate counter measures, the effects of mislead have been shown to dramatically decrease network performance. Depending on the proportion of misleading nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of mislead can endanger the functioning of the entire network. The mobility nature of the nodes in dynamic nature is also a concern in adhoc deployment. As each node travels in multiple directions the probability of nodes going out of the network is very high. This result in breakdown of the communication. Hence overall for providing an efficient performance in adhoc network a reliable, long lasting and connective routing scheme is to be developed so as to make the adhoc network a reliable wireless communication mode for next generation communication. In the need of communication, among various mode of routing, the node property controls the flow of data, by defining an optimal route. As an evolving mode of communication for long range communication, Adhoc network has come out as a very effective mode of communication. Due to non-dependency on infrastructures such networks are very rapidly emerging. While adhoc network has high portability in communication due to its self-generating properties, such network is limited with the selection of routes and their offering properties. However various researches were made to outline an efficient routing protocol for progressive data transfer in Mobile Adhoc network. In various approaches of route discovery in adhoc network, routing with security concern is upcoming. In such a network where each node is an active participant, with the possibility of entering and leaving the network at any instance, reliability over the node for communication plays an important role. In various securities based routing approaches Reliability is provided to provide security at each node level. Anonymous routing provides security by hiding node identities preventing traffic attacks from external nodes. Reliability is provided to the transferring data, source, destination identity and forwarding route.

2.1 Back ground

Research on AdHoc network has resulted in number of routing protocols suitable for MANET's. Most of this research was performed on topology based routing protocols and are generally classified as on-demand and table-driven. Among these two on-demands has gained more attention because of its lower complexity. Meanwhile position/location based routing protocols are the good alternative to on-demand routing protocol. In such a routing node's geographical position are used to make the routing decisions, resulting in improved efficiency and performance. Though the problem associated with this topology based routing protocols is, they didn't consider the security issues, such that vulnerable to number of attacks including impersonation, modification and also fabrication. In addition these protocols lack cryptographic functions, revealing the exact position information to the nodes in the range. In highly-risk environments these revealing of data are not acceptable. So the position information of such nodes need to be hidden.

2.2 Related Work

Towards developing secure routing in adhoc network, various routing protocols were developed in past. These approaches were developed with the objective of providing security wrt., data authentications, resource utilization and security provisioning with route security using node characteristics. These past developed approaches are as presented below.

2.2.1 Data Authentication Approach

Security could be defined in two approach in adhoc network. The security issue in networks, is carried out at data level, using authentication schemes, or at link level developing reliable routes, which has higher reliability. Towards providing security in data exchange level, in [1] a Key management for secure data routing is presented. The presented secure routing ensures successful routing among authentic nodes with adversary nodes existing around or inside the network, and forms the base of a secure MANET system. A key management scheme without interdependency cycle was presented. In such coding the key distribution is non-centralized However, the main concern of such a scheme is the lack of efficient locality awareness since the node regions are randomly assigned. In [2] to achieve the security factor, a threshold cryptography based on decentralized access control mechanisms for ad hoc network is proposed. This proposed approach includes access control mechanisms and the issues of group security policy in Adhoc network. However the work is concerned only with access control and does not address the specification and negotiation of group security policy. Though various keying mechanism or authentication schemes were developed they suffer from a problem of distributed architecture and imbalance usage of storage resources. The authentication at data level provides an approach to secure coding in adhoc network. However, the security provisioning at route level, based on resource utilization and security provisioning were also developed.

2.2.2 Secure Routing Protocols

(a) Security Provisioning

In [3] a security protocol termed as PRISM is proposed. In this approach tracking-resistant techniques for MANETs is developed. such techniques offer a privacy approach, since they depend on certain environmental factors, such as network size and pervasive mobility. In this case the nodes are communicated with routing of AODV scheme and a secure group signature scheme is used with defined location information. This approach provides a suitable method to deny location tracking hence source identification. In contrast the method described in [4] considers a threat as a global, passive and external eavesdropper is realistic. On the other hand, the problem of sink location privacy in this stronger notion has not

been studied. The threat model assumes that the attacker does not have global information about the whole network. To achieve the security goals, [5] proposed a hierarchical identity-based signature scheme to generate location-based signature for providing location assurance and use pseudonym-based anonymous authentication scheme for privacy preservation. In this method the two security identities are however not bonded resulting in attack higher attack probability. In [6], an open-source software solution was proposed for security provision during content sharing in mobile wireless ad hoc networks. It proposed a BitTorrent variant called BitHoc, adapted to the wireless ad hoc network environment. This architecture consists of two main components: a membership management service (BitHoc Tracker) and a content sharing service (BitHoc client). To ensure content sharing, the BitHoc client decides in a distributed manner, using routing information, of the structure of the data exchange overlay. In regard of security and Reliability provision [7] also makes two contributions. First, it shows how to obtain privacy-friendly on-demand location centric MANET routing. By "privacy-friendly" we mean resistant to node tracking by both outsider and insider adversaries. Moreover, this is achieved without sacrificing security. [8] Proposed a method to measure the popularity of any hidden service without the consent of the hidden service operator. It was shown how connectivity to selected hidden services can be denied by impersonating all of their responsible hidden services directories. Mobile social networks representing a promising cyber-physical system was suggested, which connects mobile nodes within a local physical proximity using mobile smart phones as well as wireless communication. In mobile social networks, the mobile users may, however, face the risk of leaking their personal information and location privacy. In addition the approach proposed in [9] offers protection against passive and active insider and outsider attacks. This is based on aid of advanced cryptographic techniques for an example group signature; ALARM provides both security and privacy features, including: node authentication, data integrity, Reliability and untraceability tracking resistance. It leaks quite a lot sensitive privacy information-network topology, location of every node is the major drawback. In [10] a low latency model was proposed. It first modeled the secure friend discovery process as a generalized privacy- preserving interest and profile matching problem. During this a new security threat arising from existing secure friend discovery protocols, coined as runaway attack, which can introduce a serious unfairness issue was found. [11] Contributions a threefold approach to enhance the security provision in MANETs. First, a security framework was proposed as a definition for the OR methodology as an ideal functionality for in the UC. After that, it gives corresponding security definitions: a one-way authenticated key exchange (1WAKE) primitive, and onion construction and processing algorithms. In [12] an intelligent routing scheme based on pheromone based ant routing scheme was presented. The pheromone-based ant routing algorithm is a distributed routing algorithm with good scalability and robustness. It has been shown that the procedure of establishing a stable route is self-organized towards the attractive peculiar state, and for the routing establishment is power-law distributed. To cope with real-world routing dynamics, [13] proposed a secure neighborhood-based FL protocol, DynaFL, with no requirements on path durability or the source node knowing the outgoing paths. In geocast routing approaches based on flooding are unscalable due to the high load they generate. Scalable approaches, on the other hand, have trouble in complex environments, lacking sufficient intelligence about the necessary directionality of packet flow.

(b) Routing Protocol

In [14] the author develop a new position based routing protocol named as anonymous on-demand position based routing protocol (AO2P) is developed. In this AO2P the position of the destination is encrypted with a common key of nodes, and this encrypted information is used for routing. For this purpose a route request packet has to be sent towards the position of destination from source. However, it is not so practical for each node to enforce privacy policies in ad hoc networks. So privacy preserving approaches based on centralized control become not suitable in this context. To achieve similar objective in [15] an anonymous routing protocol, ARAKE, which not only makes the sender and the receiver anonymous but also hides the intermediate nodes from the network simultaneously is defined. To make the protocol more practical in dynamic network, this protocol uses the public key to substitute the shared secret. In ARAKE, the receiver can authenticate the sender and gets a shared secret without extra key establishment processes. This approach is very robust to route attack. In [16], a reliable and efficient anonymous secure routing protocol was proposed for MANET, in which the communicating parties can select the most reliable route based on a trust relationship among nodes and then feedback the connection experience to maintain the relationship. The security works are essentially different approaches to achieve the same purpose. Besides, an efficient routing protocol that has both strong security and high network performance is considered. In [17] a passive attack approach for identified with invariant node ID is proposed. In this work a novel anonymous on-demand routing protocol, called MASK, which can simultaneously achieve anonymous MAC-layer and network-layer communication is presented. This approach use dynamic pseudonyms rather than static MAC and network addresses. However in this approach on run attacks are not resolved. As well in such approach it is observed that a probability of computational effort is higher as the security concern two factors for securing. In [18],[19] the Reliability requirements for cooperative cache based data access in MANETs is presented, and two efficient anonymous cooperative cache based data access schemes is proposed. This scheme is based on onion message and pseudonym-based encryption, respectively. The proposed schemes cannot only protect confidentiality of sensitive cache data but can also protect privacy of nodes and routes. On-Demand routing is one of the famous routing protocols used for several years. [20] Proposed ODAR, an On-Demand Anonymous Routing protocol, which provides node, link and path anonymities in ad hoc networks based on Bloom filters. The use of Bloom filters additionally gives ODAR the storage-, processing- and communication-efficiencies, making it suitable in the ad hoc network environments. The proposed design in [21] serves to bridge the gap between communication systems that provide strong Reliability protection but with intolerable latency and non-anonymous communication systems by considering a new design space for the setting. Energy based AODV protocol (EN-AODV) was suggested in [22]. This approach is

developed based on nodes sending and receiving rates and the sizes of the data to be transmitted it justifies whether its energy level is maintained or decreased. It calculates the energy levels of the nodes before they are selected for routing path. A threshold value is defined and nodes are considered for routing only if its energy level is above this threshold value. To avoid such limitation in [23] a secure, efficient, and fully non interactive admission protocol for temporary MANETs is presented. It is constructed using secret sharing techniques based on bivariate polynomials. A technique for setting up on-the-fly secure communication channels among MANET nodes is presented. In this approach a public key operations without any node certificates is presented. This is achieved by using verifiable polynomial secret sharing as a key distribution scheme and treating secret shares as private keys. In [24] a lightweight protocol for securing route establishment, data transmission, and preserving users privacy in hybrid ad hoc wireless network is presented. In this approach to preserve users' Reliability, each node uses pseudonyms and one-time session key. However the key allocated are one-time session key used hence the probability of attacks increases. To avoid such probabilities in [25] a lightweight privacy-preserving on demand routing protocol to achieve *source Reliability* and *routing privacy is proposed*. The approach is based on reactive source routing, where a route is obtained only when there is a demand to send a message. This approach reduces the network overhead, however the dynamic key selection leads to a question on its suitability. As the keys are dynamically selected the validation of the key for non-repeating or security factor is not investigated. In [26] to achieve a similar objective of higher data transmission, a load balancing ad hoc on demand distance vector (LB-AODV) protocol is proposed to avoid network congestion while considering a non-ideal transmission bandwidth. A routing metric to indicate the load condition of a path is designed. To thwart new threats, [27] introduced a novel blind vector transformation technique, which could hide the correlation between the original vector and transformed results. Based on this, a privacy- preserving and fairness-aware interest and profile matching protocol was proposed, which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa.

(c) Location Oriented security coding

To eradicate such problem in [28] a location cloaking on geographic ad hoc routing protocols is proposed. A new concept called *safe link* is introduced. To verify if a link is safe or not, a node receiving a packet needs to check if the cloaking region it discloses is completely covered by the sender's transmission range. However in such coding approach the location radius is concerned and packets are forwarded only when nodes are in contact, this leads to minimization in network throughput and overhead increases. In [29] a location service management protocol called modified region-based location service management protocol (MRLSMP) is presented. MRLSMP aims to investigate the effect of deploying a self-organized framework for managing the location information using message aggregation enhanced by geographical clustering. To overcome such issues in [30] a novel methodology to address the load balancing problem is addressed. Instead of changing the geo-routing protocol, is computed with a proposed hash function to compute the likelihood of being the destination of a query results in the desired destination density. Different load balancing approach, based on an iterative heuristic that repeatedly changes key ranges assigned to nodes as long as a load balancing metric is improved is proposed. To achieve a similar objective in mobility condition in [31] routing protocol utilizing the location information of nodes from positioning systems such as GPS is proposed. As a prerequisite of geographic routing, each node in the network must be able to determine the position of the target node it wants to communicate with. In such a coding, the location information are shared based on the broadcasting of node identities. In such an approach the broad casting overhead is neglected. This distribution builds security trustiness as the identifications are shared however the network route overhead is heavily increased. In [32] a novel tree-based diversionary routing scheme for preserving source location privacy and maximizing network lifetime in Wireless Sensor Net-works referred as the tree route, TR is presented. This approach is as well, a routing security method which maximizes the network life time by evaluating the redundant information and in accordance code for tree routing to achieve longer operational life. A novel distance-based local geocasting scheme for a multi-hop wireless network is proposed in [33], which does not require the nodes to know their geographic location information. In this approach blind flooding within the target geocasting region is presented. This is focused to reduce the broadcasting effort. [34] Defines a novel geocast heuristic, the Center Distance with Priority (CD-P) Heuristic, which both significantly improves on reliability of existing scalable geocasts and yet also remains scalable as scenario complexity increases. It also describes the new technique as well as an evaluation study comparing it to previous approaches, Source location privacy and sink location privacy are also important to increase the security enhancement in modern MANETs. The proposed approach in [35] first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. Two techniques to provide location privacy to monitored objects (source-location privacy)—periodic collection and source simulation—and two techniques to provide location privacy to data sinks (sink-location privacy)—sink simulation and backbone flooding is proposed. These techniques provide trade-offs between privacy, communication cost, and latency.

(d) Resource optimized secure route coding

In [36] the problem of using a single-radio interface for both data and control message exchange is focused. The key problem focused was to control message must be broadcasted to all available channels, which is time consuming and increases the network overhead. To overcome this problem a new routing protocol, called the spectrum and energy-aware routing (SER), for CR ad hoc networks is proposed. However in such approach the usage of primary and secondary users spectrum allocation is isolated from the derived power level for it. In [37] In addition to power allocation a route selection approach is performed at the destination. It is a hybrid approach of routing where PUs and SUs are together used for route establishment. This introduces initial delay at route establishment. In [38] Channel assignment and routing in cognitive radio networks using a combined framework of routing and channel assignment is proposed. A joint cross-

layer routing/ channel assignment protocol based on AODV that works without any central control channel is proposed. In this approach, a backup of channel is kept to cater for channel heterogeneity thereby avoiding end to end reroute procedures. However the overhead is increased. For the accurate and reliable tracking of small scale mobile PUs in CRNs an RSS based tacking approach is proposed called SOLID is proposed in [39]. The approach uses a shadowing fading approach to accurately detects both manipulated and erroneous sensing reports, thus achieving high robustness. The key motivation behind exploiting temporal shadowing correlation in attack detection is that malicious sensors cannot control the physical layer signal-propagation characteristics. A spectrum-active devices that can be programmed to operate on a wide spectrum range and tuned to any frequency band in that range with limited delay was suggested in [40]. The approach is an effective mode of spectrum utilization process wherein PU and SU can completely change their transmitter parameters. However in such approach the operational characteristic for data forwarding is not considered. In most of the security approaches or resource utilization approaches presented, focus is made on the privacy of data, but node trustiness is not evaluated.

(e) Characteristic based routing

In [41] a trust based routing for threat based routing is proposed. The proposed model evaluate the trustiness of the route to provide higher reliability in the routing. The approach of trust based coding was develop to offer higher reliability in data exchange, with the node characteristic analysis for data exchange. The operational characteristic of intentional and non-intentional characteristic analysis were not focused. Towards trustiness coding in distributed networks a framework is outlined in [42]. By investigating correlations and differences of establishing trust in social context the trust in distributed network is made and trust metrics are developed. The process of trustiness presented is based on the content of the data; however the security concern due to geographical location is not evaluated in such approach. [43] Focused on the evaluation process of trust evidence in ad hoc networks, i.e., focusing on the trust metric itself. The main contribution made in such approach is development of an algorithm with no pre-established infrastructure, with evidence in uncertain and incomplete format, and the trust metric imposing unrealistic communication/computation requirements. To achieve such objective in [44] a novel secure privacy preserving architecture has been proposed. This architecture includes the concept of observer obscurity to provide privacy and security for the genuine nodes and to exclude misbehaving nodes in the network. A misbehaving node is categorized as outlier, who drops the data packets instead of forwarding or malicious, who does not send cooperation message, upon receiving a caution. These nodes are detected or eliminated based on thresholding method. [45] Considers the mobility and proposed a novel approach for multihop network to analyze the behavior of network under insecure conditions. To provide nodes with trust relationship a trustworthy neighbor and node mobility. An interaction of node mobility in order to scale on mobility node is outlined as a tradeoff between the efficiency of trade off between the node mobility and the trustiness. In [46] mobile social networks with multiple participants holding multiple identities is addressed. The approach of pseudonymous personas, reliable and trustworthy mechanism for reputation transfer (RT) from one person to another was suggested. Such a reputation transfer model must preserve privacy and at the same time prevent link ability of learners' identities and persons.

3. Conclusion

For the past development it is observed that, approach of secure routing is a prime requirement in wireless adhoc network. To make the routing reliable a robust routing scheme is required. The network should not rely on the route developed at the route establishment stage, however should also be adaptive during communication phase. In the process of route establishment or selection intelligence logic with node characteristic should be evaluated. The nodes should be overcoming the issue of data privacy and reliable routing in concern to data forwarding, communicating and retaining of demanded quality of service in such network. The advancement of intelligent logic to the routing scheme will be an added advantage to the routing scheme.

4. References

[1] Shushan Zhao, Robert D. Kent, Akshai Aggarwal, "An Integrated Key Management and Secure Routing Framework for Mobile Ad-hoc Networks", International Conference on Privacy, Security and Trust, 2012.

[2] Nitesh Saxena a, Gene Tsudik b, Jeong Hyun Yi, "Threshold cryptography in P2P and MANETs: The case of access control", Elsevier,2007.

[3] Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal On Selected Areas in Communications, Vol. 29, No. 10, December 2011.

[4] Kemal Bicakci, Ibrahim Ethem Bagci, and Bulent Ta, "Lifetime Bounds of Wireless Sensor Networks Preserving Perfect Sink Unobservability", IEEE Communications Letters, Vol. 15, NO. 2, February 2011.

[5] Youngho Park and Kyung-Hyune Rhee, Chul Sur, "A Secure and Location Assurance Protocol for Location-Aware Services in VANETs", International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011.

[6] Amir krifa, Mohamed Karim sbai, Chadi barakat, Thierry turletti, "BitHoc: A content sharing application for Wireless Ad hoc Networks",IEEE, 2009.

[7] Karim El Defrawy and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs" IEEE journal on selected areas in communications, vol. 29, No. 10, december 2011

[8] Alex Biryukov, Ivan Pustogarov, Ralf-Philipp Weinmann, "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization", IEEE Symposium on Security and Privacy, 2013.

[9] P. Thamizharasi, D.Vinoth, "Unobservable Privacy-Preserving Routing In MANET", International Journal of Emerging Science and Engineering (IJESE), Vol-2, Issue-3, January 2013.

[10] Haojin Zhu, Suguo Du, Muyuan Li, And Zhaoyu Gao, "Fairness-Aware and Privacy-Preserving Friend Matching

Protocol in Mobile Social Networks", IEEE Transactions on Emerging Topics in Computing, 2013.
[11] Michael Backes, Ian Goldberg, Aniket Kate, "Provably Secure and Practical Onion Routing", Computer Security Foundations Symposium,IEEE, computer society, 2012.
[12] Zhang Lin, Ren Yong, Shan Xiuming, "Pheromone-Based Ant Routing System for IP Networks", Tsinghua Science and Technology, pp213-218 Volume 9, Number 2, April 2004.
[13] Xin Zhang, Chang Lan, Adrian Perrig, "Secure and Scalable Fault Localization under Dynamic Traffic Patterns", IEEE Symposium on Security and Privacy, 2012.
[14] Xiaoxin Wu and Bharat Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol", IEEE transactions on mobile computing, vol. 4, No. 4, July/august 2005.
[15] Wei Yuan, "An Anonymous Routing Protocol with Authenticated Key Establishment in Wireless Ad Hoc Networks", International Journal of Distributed Sensor Networks, Volume 2014.
[16] Min-Hua Shao and Shin-Jia Huang, "Lightweight Anonymous Routing for Reliability in Mobile Ad-Hoc Networks", Journal of Research and Practice in Information Technology, Vol. 41, No. 2, May 2009.
[17] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, Vol. 5, No. 9, September 2006.
[18] Chang-Ji Wang, Xi-Lei Xu, and Dong-Yuan Shi, "Two Anonymous Cooperative Cache-Based Data Access Schemes in Mobile Ad Hoc Networks", International Journal of Distributed Sensor Networks, 2013.
[19] Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs," IEEE Journal on selected areas in Communication, Vol. 29, No. 10, 2011 pp. 1926-1934.
[20] D. Sy, R. Chen, and L. Bao, "ODAR: On-Demand Anonymous Routing in Ad-hoc Networks," in IEEE Conference on Mobile Adhoc and Sensor Systems., vol.4, 2006, pp. 721-730.
[21] Michael Z. Lee, Alan M. Dunn, Brent Waters, Emmett Witchel, Jonathan Katz, "Anon-Pass: Practical Anonymous Subscriptions", IEEE Symposium on Security and Privacy, 2013.
[22] S.Sridhar, R.Baskaran, P.Chandrasekar, "Energy supported AODV (EN-AODV) for QoS routing in MANET", The 2nd International Conference on Integrated Information, Procedia - Social and Behavioral Sciences 73, 294 – 301, Elsevier, 2013.
[23] Nitesh Saxena, Gene Tsudik, and Jeong Hyun Yi, "Efficient Node Admission and Certificate less Secure Communication in Short-Lived MANETs", IEEE Transactions on Parallel And Distributed Systems, Vol. 20, No. 2, 2009.
[24] Mohamed M. E. A. Mahmoud, Sanaa Taha, Jelena Misic, and Xuemin Shen, "Lightweight Privacy-Preserving and Secure Communication Protocol for Hybrid Ad Hoc Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, IEEE, 2013.
[25] Liu Yang, Markus Jakobsson, Susanne Wetzel, "Discount Anonymous on Demand Routing for Mobile Ad hoc Networks", Proc. IEEE, 2006.
[26] Haina Ye, Zhenhui Tan, Shaoyi Xu, Xiaoyu Qiao, "Load Balancing Routing in Cognitive Radio AdHoc Networks", IEEE, 2011.
[27] Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Akira Yamada, "LAP: Lightweight Anonymity and Privacy", IEEE Symposium on Security and Privacy, 2012.
[28] Toby Xu, Ying Cai, "LSR: A Location Secure Routing Protocol for Ad Hoc Networks", Proc. IEEE Conf, 2010.
[29] M. Elena Renda, Giovanni Resta, and Paolo Santi, "Load Balancing Hashing in Geographic Hash Tables", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, no. 8, August 2012.
[30] Hanan Saleet, Rami Langar, Otman Basir, and Raouf Boutaba, "Proposal and Analysis of Region-based Location Service Management Protocol for VANETs", proceedings of IEEE "GLOBECOM", 2008.
[31] Jun Long, Mianxiong Dong, Kaoru Ota, Anfeng Liu, "Achieving Source Location Privacy and Network Life-time Maximization through Tree-based Diversionary Routing in Wireless Sensor Networks", IEEE ACCESS, 2014.
[32] Quan Jun Chen, Salil S. Kanhere, Mahbub Hassan, Yuvraj Krishna Rana, "Distance-based Local Geocasting in Multi-hop Wireless Networks", proceedings Of IEEE, WCNC 2007.
[33] Robert J. Hall, "An Improved Geocast for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 10, No. 2, February 2011.
[34] Kiran Mehta, Donggang Liu, and Matthew Wright," Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE Transactions on Mobile Computing, Vol. 11, No. 2, February 2012.
[35] S.M. Kamruzzaman, E. Kim, D.G. Jeong, W.S. Jeon, "Energy-aware routing protocol for cognitive radio ad hoc networks", IET Communications, 2012.
[36] Nitul Dutta, Hiren Kumar Dev Sarma, "A Routing Protocol for Cognitive Networks in presence of Co-Operative Primary User", IEEE, 2013.
[37] Muhammad Zeeshan, Muhammad Fahad Manzoor, Junaid Qadir, "Backup Channel and Cooperative Channel Switching On-Demand Routing Protocol for Multi-Hop Cognitive Radio Ad Hoc Networks (BCCCS)", ICET, 2010.
[38] Alexander W. Min, and Kang G. Shin, "Robust Tracking of Small-Scale Mobile Primary User in Cognitive Radio Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, April 2013.
[39] Ian F. Akyildiz, Won-Yeol Lee, Kaushik R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks", Elsevier, 2009.
[40] Todd R. Andel, Alec Yasinsac, "Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols", Electronic Notes in Theoretical Computer Science 197, 3–14, Elsevier, 2008.
[41] Yan Lindsay Sun, Zhu Han, Wei Yuand K. J. Ray Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks", in the proceeding of IEEE INFOCOM, 2006.
[42] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 318:328, Feb,2006.

[43] Muthumanickam Gunasekaran and Kandhasamy Premalatha, "SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking, 2013.
[44] Velloso P. B, Laufer R. P, Duarte O. C. M. P, and Pujolle G, "Analyzing a human-based trust model for mobile ad hoc networks," in IEEE Symp. Computing Communication, Marrakech, Morocco, July 2008.
[45] Haojin Zhu, Suguo Du, Muyuan Li, And Zhaoyu Gao, "Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks", IEEE Transactions on Emerging Topics in Computing, Vol. 1, No. 1, June 2013.

Author Profile

Ugendhar Addagatla presently working as Associate professor in the department of Computer Science and Engineering at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Hyderabad, Telangana State, INDIA. He has 12 years of teaching experience. He is associated with ISTE and CSI as life member. He has obtained B. Tech. degree in Computer Science and Engineering from Christu Jyothi Institute of Technology and Science, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2003, M.Tech. degree in Software Engineering from Ramappa Engineering College, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2008 and my area of Research interest is Mobile Computing, Ph.D (CSE) from Jawaharlal Nehru Technological University, Hyderabad and it is my part of Research work.

Dr. V. Janaki received Ph.D degree from J.N.T. University Hyderabad, India in 2009 and M.Tech degree from R.E.C Warangal, Andhra Pradesh, India in 1988. She is currently working as Head and Professor of CSE, Vaagdevi Engineering College, Warangal, India. She has been awarded Ph.D for her research work done on Hill Cipher. Her main research interest includes Network security, Mobile Adhoc Networks and Artificial Intelligence. She has been involved in the organization as a chief member for various conferences and workshops. She published more than 50 research papers in National and International journals and conferences. She is presently supervising nearly 10 scholars for their research.