Anonymous Routing Protocol with Multiple hops for Communications in Highly Dynamic Hetrogenious Networks

Vikram Neerugatti, A Sreekanth Reddy, Varam Deepa.

Abstract

Mobile ad hoc networks (MANETs) are increasingly adopted in both military and civilian usesdue to its self configuration and self-maintenance capabilities. MANETs are higly vulnerable to security threats due to inherent charateristics as wireless transmission , lack of fixed infrastructure , dynamically changing topoly, etc. The broadcast nature of the wireless medium makes MANETs susceptible to various malicious attacks. Traffics annalsis is one of the most serious security attacks in MANETs. For instance , in a battle field the enemy can physically destroy the important mobile nodes if they can identify and locate suck nodes by traffic analysis . In order to thwat such attacks , ananymous communication protocols are developed. For the purposes of security and robustness , an ideal anonymous routing protocals as in the route, in particular , those of the source and the destination. Multiple routes should be established to increase the difficulty of traffic analysis and to avoid broken paths due to node mobility . Existing schemes either make the unrealistic and undesired assumption that certain topological information about the network is known to the nodes , or cannot achieve all the properties described in the above .

In the paper , we propose an anonymous routing protocol with multiple routes called ARMR, which can satisfy all the required properties. In addition, the protocal has the flexibility of creating fake routes to confuse the adversaries , thus increasing the level of anonmity. In the terms of communication efficiency , extensive simultion is carried out. Compared with AODV and MASK , our ARMR protocol gives a higer route request success rate under all situations and delay of our protocol is comparable to the best of these two protocols.

Keywords –MANET, Secure Routing, Anonymous Routing, ARMA Protocol, Traffic Anonymity, Data Anonymity.

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) consist of a collection of wireless mobile nodes to form a network that does not need any pre-deployed infrastructure and routing packets are transmitted only relying on the intermediate peers. One of the aims of MANETs is to turn the dream of making users get connected at anytime and anywhere into true. Due to the attractive characteristics of MANETs, many practical applications are being designed including military and civilian scenarios. Typical application examples include military battlefield operations, disaster rescue scenarios, and ad hoc meetings, among others [1]. When planning mobile ad hoc networks, security is indispensable because of the shared nature of wireless devices, the mobility of the nodes and the limited transmission range.

Adhoc means in Latin "formed for" or "concerned with one specific purpose", nodes in Ad

ISSN: 2278 – 1323

HocNetworks are freedom to move, they may act as both host and router, and each node can be trust traffic on anther nodes maintaining connectivity in a decentralized manner. That's why Ad hoc Network is also known as infrastructure less network, also nodes are self-forming and self-configuring.[2], [3]. It has many characteristic that differentiate it from other wireless network include: Dynamic deployment, Wireless medium less dependable than wired medium, Limited Capacity and Bandwidth, Energy life in mobile node power resources can be replaced by users, and the Security because mobile nodes in the network its prone to many kind of attacks [4]. Routing protocols for Mobile Ad Hoc Networks is very important to ensure deliver packet to appropriate destination it can be classified to: (i) Table Driven or Proactive Protocols is updated every time the topology changes [5]. (ii) On Demand or Reactive Protocols is obtaining to create a path to a destination only when node in the network demands for it [6]. (iii) Hybrid Routing Protocols in this type is mixed between the above types [4]. Although all these routing protocols for Mobile Ad Hoc Networks without any protect from any type of attack. We used Cryptography for improve security to AODV protocol. Cryptography is an operative method of defensive sensitive information as it is kept on media or transmitted through network communication routes. The main reason for use cryptography for hide information from anyone unauthorized those called attackers, if the attacker has enough time, desire, and resources the algorithms can be destroyed and the information can be exposed [7]. Cryptography can classified into two type: secret key is also known as symmetric cryptography is single key used for both encryption and decryption but the major difficulty with this method is the distribution of the key that it's solved by the another type is public key (asymmetric) cryptograph public cryptography [8]. The uniformly distributed keys in encryption and decryption it's the same between communication parties the authentication can only be achieved for that reason public-key cryptography is used to solve the problem of key agreement or distribution, this render public key more suitable for MANETs. Nonetheless the Traditional public key cryptography usually used when dependence on a Public Key Infrastructure (PKI), that means it has a Certificate Authority as principal control point that every node in MANET must be trusted in this point. That is a big obstacle with the MANET characteristics also this PKIs make MANETs is more overhead in storage and packet transmission.

In the MANET, the DSR[16] and AODV[14] are two principal on-demand routing protocols. However, they do not provide any security and anonymity protection, which make them vulnerable to a variety of security attacks. Up to now there have existed a number of valid and novel MANET anonymous routing protocols [9-13]. We classified them into two types based on their routing method. One is similar to the DSR routing protocol, the other is similar to the AODV routing protocol. The idea of ANODR[9], ASR[10] and MASK[11] is similar to AODV routing protocol which the intermediate node only know the previous and next node information ,and the source and destination node needn't know the whole nodes en route. The overhead of packets forwarding in these protocol don't contain the whole route information. In the other side, the idea of SDDR[13] and AnonDSR[12] is similar to DSR without optimization, in which the source node store the route to the destination node and the nodes en route don't store the path information. The overhead of packets forwarding in AnonDSRprotocol contain the whole route information.

ISSN: 2278 – 1323

In[18],the author perfected the ANODR which was firstly proposed in [9] and provided better solutions for route discovery, data transfer and route maintenance. They also analysed more comprehensively on the anonymity and security properties. The advantage of ANODR is trapdoorboomerang onion (TBO) used in route discovery which can protect the anonymity of node en route and destination node.

The trapdoor thought is also accepted by the later anonymous routing protocols. To reduce the public key cryptographic computation, they advised the correspondence nodes exchange the symmetric key in the first route discovery. Then, the source would use the symmetric key in later route discovery processes toward the same destination node. However, one limitation is that the public key algorithms have to be processed in the RREP packets during route discovery. The other limitation of the protocol is the symbol of RREP in REEP packet may leak the route information due to its unicast mode.

MASK uses periodic hello messages to establish pairwise trust relationship between neighbourhood nodes when the nodes move to the new place. Like ANODR, MASK employs an on demandprocedure to establish a virtual circuit for later data delivery. The limitation of MASK is that it provides conditional destination anonymity by utilizing and exposing the destination's identifier in ARREQs which it will benefit to get much better routing efficiency. The MASK doesn't introduce the trapdoor thought used in ANODR.

AnonDSR and SDDR are anonymous routing protocol based on the mix-net [15] layer-encryption thought and the DSR protocol thought. They use layer encryption like onion in RREQ phase and each node en route will use the temporal public key to encrypt their pseudonym and symmetric key to encrypt the onion. As the destination node decrypts the trapdoor, he will also decrypt the onion and get the intermediate node's pseudonym and corresponding symmetric key which won't expose the intermediate nodes true identity. After destination node return RREP to source node, the source and destination nodes can communicate anonymously as the TOR[17]. To avoid running the public key decryption on the trapdoor which will cost too much time and power on mobile nodes, the AnonDSR introduces a security parameter establishment (SPE) protocol to manage shared secrets between end-nodes and the global trapdoor in RREQ is encrypted using symmetric cryptography. The one limitation of AnonDSR is that it may leak the route information during AnonDSR's SPE phase because the route discovery in SPE phase is not encrypted and theroute in SPE phase may besimilar to the route in the anonymous route discovery. The other limitation is it doesn't support the bi-directional link inthe data transferred phase.

In the paper , we propose an anonymous routing protocol with multiple routes called ARMR, which can satisfy all the required properties. In addition, the protocal has the flexibility of creating fake routes to confuse the adversaries , thus increasing the level of anonymity for MANETs which can overcome the shortcomings of above anonymity routing protocol and provide an efficient, security, strong anonymity, widely adaptability communication protocol for the routing establishment and data forwarding.

The rest of the paper is organized as follows. Section II presents the related work. Section IIIpresents our anonymous targets and the network assumptions and attack models. Section IVdescribes the essential idea of anonymous routing ARMRand the detail implementation of routing protocol. We present Proof of Correctness

ISSN: 2278 – 1323

in section V. Section VI presents some concluding remarks in the paper.

II. RELATED WORK

The limited resources of wireless devices in MANETsrequiring an efficient and reliable routing strategy become a quite challenging issue. Papadimitratos and Hass have proposed a Secure Link State Routing Protocol (SLSP) to secure the proactive topology discovery. The nodes of SLSP maintain and disseminate the updated topological information within their own zones in term of *R* hops. Smith *et al.* have presented a solution to the security problems of distance-vector protocols that use two classes of protection mechanism respectively for routing messages and routing updates.

Hu *et al.* present a Secure Efficient Ad hoc Distance vector routing protocol (SEAD), which employs one-way hash functions instead of asymmetric cryptographic encryption. Papadimitriou and Haas also propose SRP (Secure Routing Protocol) based on DSR . The protocol introduces an effectively secure query/reply mechanism to prevent the misbehaviour of malicious nodes. Sanzgiri*et al.*propose the ARAN (Authenticated Routing for Ad hoc Networks) protocol that makes use of cryptographic certificates to offer routing security. Hu *et al.*provide a new secure on-demand ad hoc network routing protocol (Ariadne), where routing messages are authenticated to use different encryption approaches. Awerbuch*et al.*discuss the issue of byzantine failures and propose an on-demand routing technique to detect a malicious link.

Secure routing in the Internet has received increased attention, while secure routing for ad hoc networks is important too. Some research has been developed for the anonymity for these networks. Onion Routing protects the privacy of the sender, the receiver, message content as a message is traversed to a network. SDAR proposed byBoukerche*et al.* is a novel secure distributed anonymous routing protocol that uses onion routing to protect the anonymity and location of communicating nodes and introduces trust management system to filter those untrustworthy nodes. Kong *et al.* DesignAnonymous On-Demand Routing (ANODR) which is based on a novel network security concept: “broadcast with trapdoor information”. Zhang *et al.*design anonymous on-demand routing protocol to authenticate the anonymous neighbourhood nodes and establish the anonymous route discovery by pairing technique. Liu *et al.*describe their trust management scheme for trust-based multi-path routing, where honest nodes receive the credit for good behaviour; however, suspicious nodes will be penalized if they supposedly lie about or exaggerate their contribution to routing.

MANETs was derivation through the military, define by the Defence Advanced Research Projects Agency (DARPA) that supported packet radio (PRNET) networks in 1970s, then still developing until Ad Hoc Networks entered a new stage of growth due to the popularity and the idea of an infrastructure less crew of mobile hosts was proposed, and its stall to develop. Cryptography is used to provide security goals for Ad Hoc Network because increase threats in network. Shamir was first proposed the idea of Identity-based cryptography, he proposed it can be enables any pair of nodes to communicate securely and to verify each other’s signatures without exchanging private or public keys, by calculate public key through chooses his name and network address, while secret key is computed by Private Key Generator which can be privileged situation by knowing some secret information that enable it to calculate the secret keys of all users in the network.

ISSN: 2278 – 1323

After Shamir announced his idea not developed quickly. Boneh andFranklin in 2001 proposed Identity-Based Encryption from the Weil Pairing. They offer a completely practical Identity-Based Encryption scheme (IBE) and provide accurate definitions for secure identity based encryption schemes. Adjih et al in 2005, propose secure OLSR using IBC. Their suggestion TA is in charge of certifying or assigning keys of each node joining in the trusted network. Each node sharing the network will have the public key of the TA as global key; any node entering the ad hoc network could deployment its public keys, with a specific key exchange protocol, with proper parameters and signatures. Key that used later to sign message is called the local key. A node would start creating OLSR control messages, signing them using the local key with a specific addition which prepends a special signature message.

The Routing protocols were presented for ad hoc networks deal with changing deployment of mobility nodes. Secure Routing protect against any threat on the network. The information that transmitted between mobility nodes must be route by routing protocols this information is the aim of many threats. There are twothreat types on secure routing . One came from outsidethe network called external by inserting, replaying, or distorting information. Another threat came from inside network by compromised nodes, which may it announce false information to other nodes to distinguish this information is very difficult because vulnerable nodes are capable to create legal signatures using their private keys . For protected from the first threat by using cryptographic schemes for ensure security routing information, this way is not effective for the second threat. But it not necessity to ignore this type ,the detection of compromised nodes through routing information difficult in an ad hoc network as a result of changing deployment. The routing protocol should be capable to discovery paths that go around these vulnerable nodes. Routing protocols can discover multiple directions for example protocols in DSR , AODV and ZRP , nodes that use these protocol can change to an another route when the main route appears to have unsuccessful .

III. PRELIMINARIES

Anonymity Goals

We classify into three anonymity goals proposed by asfollows:

- *Identity anonymity:*The source and destination node cannot be identified by its neighbours. And it is computationally difficult for adversaries to snoop and determine the node's true identity. These nodes needed protection include the sender nodes, recipient, nodes en route.
- *Location anonymity:* Location Privacy consists of the following requirements: (a) No one node knows the exact location of the source or the destination, except themselves; (b) Other nodes, typically intermediate nodes en route, have no information about their distance, i.e. the number of hops, from either the source or the destination.
- *Route anonymity:*Route anonymity consists of the following requirements: (a) Adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination; (b) Adversaries out of the route have no information on any node en the route.

Network assumption and attack model

We assume that all nodes are wishing to forward the packets according to the protocol and have

ISSN: 2278 – 1323

enough computational ability to process the algorithms in our protocol.

We assume that the adversaries have unbounded eavesdropping capability to overwhelm any practical security protocol but bounded computing and node intrusion capabilities

We assume that passive adversaries can communicate with each other through private and fast communication methods, either wireless or wired. They can collaborate with each other to monitor every radio transmission on every communication link. In addition, they may compromise any node in the target network to become an internal adversary.

IV. PROPOSED WORK

We propose ARMR routing protocol for MANET. It is inspired by a combination of DSR, TOR, AODV, MASK, MASR and ANODR. We find that there exist similar thoughts in DSR and TOR. For instance, the source node in these protocols should know the whole route before data transferring. And the data packets also should contain the route information overhead. The Onion Router (TOR) is the culmination of many years of research by the Onion Routing project. To protect the data and routing information, the proxy of source node constructs a multi-layer encrypted data structure called an onion and sends it through the network. Each layer of the onion defines the next hop in the route. The node en route that receives an onion peels off the topmost layer, identifies the next hop, and sends the remaining onion to the next router. From above analysis, we can utilize the DSR protocol adaptability for unidirectional link, For layer encryption method and the global trapdoor introduced by ANODR to construct our ARMR protocol.

Path Discovery Phase

The path discovery phase allows a source node *S* to discover and establish a routing path through a number of intermediate wireless nodes, in order to communicate with the destination node *R* securely and privately. When the source node *S* triggers the path discovery phase, the agent *EDA* associated with the destined node's ID and other information are included in the path discovery message that has three parts. The first part is the open part, which indicates the message type, *TYPE*, trust requirement, *TRUST_VALUE*, and a unique identifier for the message, *MESSAGE_ID*. The second part contains the mobile agent *EDA*, and the length *PLS* of the third part, padding. *EDA* includes *IDR* of the intended receiver *R*, encrypted by *EDA*. Padding *PS* generated by the source node *S* in the third part can hide real routing information and protect against message size attack. When a node *i* receives a path discovery message, it processes the message according to the steps as described in Figure 1.

Creating multiple routes with fake routes Phase

When the network is scalable or the trust value required by the source node is not high, it is possible to discover multiple different routes based on our current multicast routing strategy, so the optimal path is helpful for the latter data transfer phase. Here, we utilize the similar approach as the ARAN protocol: a non-congested, non-shortest route will likely be preferred to a congested, shortest route . This means that network congestion or network delay may lead that the first reply to the source node from a route discovery request did not travel along the shortest route. Therefore, ARMA does not seek a shortest path, but prefers a quickest path. After the source node *S* verifies that the first path discovery message is correct and valid, it then uses a similar approach to the path discovery process to transfer the official data. The sender provides the official data to the mobile agent including the information about all intermediate nodes along the established route to the receiver.

ISSN: 2278 – 1323

The official data is encrypted by the session keys provided by the intermediate nodes. Each intermediate node just decrypts the message using its session key and then forwards it to the next node according to the ID of the next node provided by *EDA* until it reaches the destined receiver.

(1) Check if the new arrived message has already been
received based on the unique identifier *MESSAGE_ID*.
If the message was received previously, drop it silently
and stop; otherwise, continue.
(2) Check if the node satisfies the required trust value.
(3) Provide its ID to the path discovery message, so that the agent *EDA* can check if the node is the destined receiver.
(4) If the node is NOT the intended receiver, then
(a) The agent *EDA* will generate a secret key *Ki* to encrypt the following information and append to the message: the identifier of the intermediate node *IDi*, a session key *SKi*generated by this node and the signature of the original received message. The key *Ki* will be stored in *EDA* so that it can be retrieved by the source or destination node to decrypt this corresponding information.
(b) Ask the node to forward the new message to its neighbors whose trust values meet the source node's trust requirement.
(5) If the node is the destined receiver *R*, then
(a) *EDA* hands over the autonomy to the receiver.
(b) The receiver implements its corresponding operations and triggers the path reverse phase.

Figure 1/path Discovery phase Algorithm.

Mobile Agent

The goal of mobile agent applied in our protocol is to protect the privacy of the communicating parties. Here, the mobile agent called Encryption and Decryption Agent (*EDA*) has two functions: (1) judge the intended destination; (2) generate different keys to encrypt the intermediate node's ID and other information. The agent is generated by the source node, and only the source and destination nodes are authorized to manage this agent after authentication. That is, all intermediate nodes cannot encrypt and decrypt any information through this agent. The advantage of mobile agent is that the autonomy of encryption is controlled by mobile agent, instead of intermediate nodes. Therefore, it is not necessary to trust each cooperating node; if one or more nodes are compromised, anonymous communication can still be achieved.

Path Reverse Phase

When the intended receiver *R* gets the path discovery message, it will implement its corresponding operations to retrieve the information about all intermediate nodes and compose the path reverse message, as shown in Figure 2.

When the source node *S* receives the path reverse message, it decrypts the two sets of encrypted information about the intermediate nodes respectively from the path discovery phase and the path reverse phase through *EDA*. After the source node obtains all IDs about the intermediate nodes, it will apply *TIP* mechanism to verify them. Thus, the source node can compare if these identifiers provided by the intermediate nodes are consistent and correct. If there is any malicious node providing incorrect or false identifier during the route establishment process, such invalid route will not be accepted by our *TIP* mechanism. Then the

ISSN: 2278 – 1323

source node *S* passes the information about all the intermediate nodes (i.e., the route) to the higher application.

(1) Decrypt the IDs of all intermediate nodes, compose a
message that contains all these IDs along the path to the source node, encrypt the message through the agent *EDA*, and then send the path reverse message back.
(2) Check if the new arrived node is along the reverse path to the source node. If not, drop this message silently
and stop; otherwise, continue.
(3) Provide its ID to the path reverse message, so that the
agent*EDA* can check if the node is the source node.
(4) If the node is NOT the intended source node, then
(a) The agent *EDA* will generate a secret key *Ki'* to encrypt the identifier of the intermediate node *Idi*again and append to the message.
(b) Ask the node to forward the new message to the next node on the reverse path.
(5) If the node is the destined source node *S*, then
(a) *EDA* hands over the autonomy to the source node.
(b) The source node applies the *TIP* mechanism and
implements its corresponding operations.

Figure 2. Path Reverse Phase Algorithm

Mobility of Nodes (capable when network breaks)

It is indispensable for routing protocols to take the mobility of nodes into account. After the route has been established, the mobility of nodes often disrupts the existing information exchange. In order to continuously communicate along the path, in our protocol we utilize the same mechanism of route maintenance as DSRand it is unnecessary to issue periodic routing updates to check for changes in the route status. When the data link is broken at a node because of the mobility of nodes or other reasons, this node will send a route error message to the source node of the route. Once the route error message is received by those nodes that detected this error node, they will remove the node in error from their route cache, and all routes through this node should be truncated there. A new route discovery request might be triggered later.

V. PROOF OF CORRECTNESS

The proposed ARMA protocol owns many different characteristics when compared to other conventional protocols.

In this section, we will provide the proof of correctness of our ARMA protocol.

Theorem 1.*ARMA is secured against passive and active attacks.*

Proof.

1. ARMA provides protection against passive attacks. This is proved based on the path discovery phase and the path reverse phase. During the two-way conversations, all identifiers *IDi*of the intermediate nodes as well as the identifier *IDS* of the source node and the identifier *IDR* of the intended receiver, are encrypted by either the public key *PKS* of the sender or the secret keys respectively generated by the mobile agent *EDA*. The session keys and other information provided by the intermediate nodes are also encrypted in the same approach. Since only the source and destination nodes can access EDA, the passive attacks can be prevented effectively. Thus, an adversary cannot learn anything information about the real sender, receiver, and all intermediate

ISSN: 2278 – 1323

nodes, even if it obtains the path discovery message or the path reverse message.

2. ARMA provides protection against active attacks. As the mobile agent technique is applied in our protocol, the source node embeds its identifier and the encryption function into *EDA*, Thus, the modification attacks cannot occur even if the malicious nodes obtain the path discovery message. In addition, the secret key generated by the agent *EDA* can protect the path discovery message against replay attacks. Given that some adversaries want to impersonate the sender or some intermediate nodes, the receiver can easily find out by *EDA*that prevents not only *malicious modification*, but also impersonation or other kinds of active attacks.

Theorem 3.*ARMA guarantees the anonymity of the sender and receiver.*

Proof.

1. During the path discovery phase: If a malicious node receives the path discovery message and only forwards it to its malicious neighbours, the path might include more malicious nodes after the first one. However, even if this case happens, our protocol can still achieve anonymity, because the information of communicating parities is encapsulated in the corresponding mobile agent, even if the path discovery request will never be sent to the intended receiver under such circumstances. The malicious nodes that obtain the mobile agent still cannot access the agent and decrypt the secret information, as only the source and destination nodes can be authenticated by *EDA* to access the agent.

If a series of nodes is compromised and the nodes can collude with each other, they would not know where the message came from and where the message was forwarded, because the destination information always was encrypted by *EDA*, and particularly, *EDA* will judge and decide if the destination arrives or not. In addition, the route reverse phase also helps to prevent node collusion attacks as the route reply mechanism means that the receiver has received the route discovery request.

2. during the path reverse phase: If a malicious node receives the path reverse message, the mobile agent *EDA* will protect the anonymous information as such information is encrypted and included in *EDA*. The same situation can happen like the above path discovery phase. If a series of nodes is compromised and the nodes can collude with each other, *EDA* still can guarantee the anonymity as *EDA* will judge and decide if the destination is reached or not.

Theorem 4.*ARMA guarantees the anonymity of the message content.*

Proof.ARMA can achieve the anonymity for the content of the message, as the message is encrypted and contained in *EDA* so that malicious nodes cannot retrieve the hiding information when they obtain the path discovery or path reverse message.

Theorem 5.*ARMA has the capability of identifying malicious nodes and establishing routes without them.*

Proof. The features of wireless ad hoc network and their bidirectionallinks among wireless nodes determine that the wireless nodes can monitor thebehaviours of their neighbouringnodes. The malicious behaviours of a node can be found by its neighbours and the malicious node can be excluded from its neighbouring community accordingly. Thereby, the neighbouringnode can accept the path discovery message but avoid the misbehaving nodes through the trust management systems.

VI. CONCLUSION

Anonymity is one of the most challenging issues in wireless and mobile ad hoc networks. In this paper, we have presented a novel secure and anonymous routing protocol for wireless ad hoc networks. Our protocol employs the technique of mobile agent to

ISSN: 2278 – 1323

dynamically discover routes without the necessity of requiring the intermediate nodes to operate the route discovery message. The identities of the sender and the receiver as well as the topology of the network are anonymous. In our approach, our protocol can prevent malicious nodes compromising the communication through collusion, and the agent obtains the autonomy of the encryption to improve the security.

REFERENCES

[1] B. Hughes and V. Cahill, “Achieving real-time guarantees in mobile ad hoc wireless networks”, 24th IEEE Real-Time
Systems Symposium, pp. 37–40, 2003.

[2] Ç. Erdal and R. Chunming, Security in Wireless Ad Hoc and Sensor Networks, 1st ed , A John Wiley and Sons, Ltd,
Publication, United Kingdom, 2009.

[3] T. Sunil and K. Ashwani,"A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of
Innovation, Management and Technology, Vol. 1, No. 3, August 2010.

[4] S. Kuldeep, K. Neha and M. Prabhakar, " An Overview Of security Problems in MANET", [Y. Hu, A. Perrig and D.
Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, inProceedings of ACM
MOBICOM’02, 2010.

[5] P. Niroj, "A secure Zone-based routing protocol For Mobile ad hoc networks", M.S. thesis, Dep. Computer Scie.,
Department of Computer Science and Engineering National Institute of Technology, India May 2009.

[6] S. Kimaya, L. Brian, S. Clay, D. Bridget, R. Elizabeth, "A Secure Routing Protocol for Ad Hoc Networks", IEEE 10 th,
International Conference on Network Protocols,2002.

[7] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol 1, No. 15,
Haryana, 2010. K. Anil and R. Sanjeev, "Identity-Based KeyManagement in MANETs using Public Key
Cryptography", International Journal of Security, Vol 3, India.

[8] S. Zhao, A. Aggarwal, R. Frost and X. Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-
Hoc Networks", IEEE Communications Surveys & Tutorials, 1553- 877X/11/$25.00, 2011.

[9] J. Kong, X. Hong. ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In
Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03),
pp. 291--302, 2003.

[10] B. Zhu, Z. Wan, M. S. Kankanhalli, and F. Bao, R. H.Deng, AnonymousSecure Routing in Mobile Ad-hoc Networks.
Proceedings of the 29thIEEE International Conference on Local Computer Networks (LCN 2004),Tampa, USA, pp.
102-108, November 2004.

[11] Y. Zhang, W. Liu, and W. Lou.Anonymous communications in mobile ad hoc networks. In Proceedings of the 24th
International Conference of the IEEE Communications Society (INFOCOM 2005).IEEE, 2005.

[12] R. Song, L. Korba, and G. Yee.AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc
Networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2005

ISSN: 2278 – 1323

[13] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Secure dynamic distributed routing algorithm for ad hoc wireless
networks," in Proc.ICPP Workshops, Kaohsiung, Taiwan, Oct. 2003.

[14] C. Perkins, E. Belding-Royer, and S. Das.Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July
2003.

[15] David Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM,
24(2), 1981.

[16] D. B. Johnson, D. A. Maltz, and Y. Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR).
<draft-ietf-manet-dsr- 09.txt>, April 2003.

[17] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The secondgenerationonion router. In Proceedings of the 13th
USENIX Security Symposium, August 2004.

[18] Kong Jiejun, Hong Xiaoyan, Gerla, M. An Identity-Free and On- Demand Routing Scheme against Anonymity Threats
in Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, Volume 6, Issue 8, Aug. 2007 :888 – 902

[19] B. Awerbuch, D. Holmer, N.-R. Cristina, H. Rubens, "An on-demand secure routing protocol resilient to byzantine
failures", 3rd ACM workshop on Wireless security, pp. 21–30, 2002.

[20] A. Boukerche, K. El-Khatib, L. Xu, L. Korba, "Performance evaluation of an anonymity providing protocol for wireless
ad hoc networks", Performance Evaluation, Vol. 63, pp. 1094–1109, 2006.

[21] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private Internet connections",
Communications of the ACM, Vol. 42, pp. 39–41, 1999.

[22] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks",
Technical Report, TR01-384, Rice University, 2001.

[23] Y.-C. Hu, D. B. Johnson, A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc
networks", 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3–13, 2002.

[24] D. B. Johnson and D. B. Maltz, "Dynamic source routing in ad hocwireless networks", Mobile Computing, Kluwer
Academic Publishers, pp. 153–181, 1996.

[25] J. Kong and X. Hong, "ANODR: Anonymous on demand routing withuntraceable routes for mobile ad hoc networks",
4th ACM symposium on Mobile ad hoc networking and computing, pp. 291–302, 2003.

[26] K. Liu, N. Abu-Ghazaleh, and K. Kang, "Location verification and trust management for resilient geographic routing",
Journal of Parallel and Distributed Computing, Vol. 67, pp. 215–228, 2007.

[27] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", SCS Communication Networks and
Distributed Systems Modeling and Simulation Conference, 2002.

[28] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", Applications and the
Internet Workshops, pp. 379–383, 2003.

[29] B. R. Smith, S. Murthy, and J. J. Garcia-Luna-Aceves., "Securing Distance-Vector Routing Protocols", Symposium on
Network and

ISSN: 2278 – 1323

Distributed System Security, pp. 85–92, 1997.

[30] K. Sanzgiri, et al., "A secure routing protocol for ad hoc networks", 10thInternational Conference on Network

Protocols, pp. 78–87, 2002.

[31] Y. Zhang, W. Liu, W. Lou, "Anonymous communications in mobile ad hoc networks", 24th Annual Joint Conference

of the IEEE Computer and Communications Societies, pp. 291–302, 2005.

Vikram Neerugatti Pursuing M.Tech., CSE (II Year), Global College of Engineering and Technology, Kadapa.

B.Tech from JNTU in 2009, M.S from BRAINWELLS UNIVERSITY, UK. in 2010. MSc Psychology from SVU Thirupathi. Having 4 Years of experience in teaching in SVCE from 2010 to till date, Area of Interesting Data Mining, Computer Networks, Android Operating systems. Attended 3 National & International Conferences. 2 international Journals, attended 4 workshops, organized 3 workshops. Guided 5 UG level projects and 3 PG level projects.

A Sreekanth Reddy, Asst. Prof., Global College of Engineering and Technology, Kadapa.

B.Tech from JNTU in 2008, M.Tech from JNTU in 2011. Having 3 Years of experience in teaching in GCET from 2011 to till date, Area of Interesting Data Mining, Cloud Computing, Big Data,Computer Networks. Attended 2 National & International Conferences, 2 journals.

Varam Deepa Pursuing M.Tech., CSE (II Year), Sri Venkateswara College of Engineering and Technology, Chittoor.

Completed M C A from Sri Venkateswara University in 2009 with 76 %, persuing M.Tech CSE in SVCET Chittoor, after MCA having 3 Years teaching Experience in MJR College of Engineering & Technology, Piler . Areas of Interest Cloud Computing , Cryptography, Algorithms Design and Analysis Process . Attended one National Conference at SVCET Chittoor in the topic of Recent Trends in Computing.

ISSN: 2278 – 1323