ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Percentage Based Trust Model with Bandwidth Reservation Technique for Privacy Preserving Routing in MANETs

Raghu. R [1], Gopinathan. B [2]
(Department of CSE, Adhiyamaan College of Engineering/Anna University, Tamilnadu, India)[1,2]

***Abstract* – Routing in Mobile Ad-Hoc Networks are vulnerable to malicious traffic analysis, harmful attackers can mitigate paths and malicious intermediate nodes breaks security, ineffective reserve of available resources (utilization of bandwidth) in node causes losses and as well as anonymity, unobservability of communication is not provided. To detect misbehaviors and effective utilization of resources in trusted nodes the Percentage Based Trust management system, with bandwidth reservation technique is proposed, and for achieving privacy in MANETs the PPRP is proposed. In this paper the scheme called Percentage based Trust management system is defined to allow trustworthy intermediate nodes to participate in path construction with resource reservation technique to allow trusted nodes to select a path which has minimum cost, congestion and bandwidth. In reservation technique, if available bandwidth is greater than traffic jam bandwidth. Using rate monitoring and adjustment methodologies, rate control is performed for the overcrowded flows and then an Privacy Preserving routing Protocol (PPRP) is proposed to offer complete anonymity, unlinkability and unobservabilty for all types of packets. PPRP uses novel combination of group signature and Id based encryption techniques for route discovery. The simulation result shows that this paper achieves trustworthy path construction through intermediate nodes with resource allocation technique and stronger privacy protection is achieved than existing scheme like AODV.**

Keywords: Routing protocols, Bandwidth, Security, Privacy, Anonymity, Unlinkability, Unobservabilty.

I. INTRODUCTION

In this paper, a secure trust construction scheme [1] is proposed. The proposed scheme does not require the source node to gather and store information about the network topology. Instead, the source node calculates cumulative trust value in node and initiates a trust establishment process by broadcasting a trust establishment message with certain trust requirements to all of neighboring nodes. Intermediate nodes satisfying these trust requirements insert their identification (IDs) and a session key into the reply message and forward copies of this message to their selected neighbors until the message reaches all selected nodes. In MANETs, ineffective reserve causes weighty losses to the service providers and results in inadequate user expertise. For improving Qos of MANETs, efficient resource allocation techniques are required. In this paper bandwidth reservation technique [2] for MANET is proposed. The source starts forwarding the packets through the trusted nodes which has minimum cost, congestion and bandwidth path. The status of every node is composed which includes the bottleneck bandwidth field and the transitional node computes the available bandwidth on the link. At the destination, after updating the new traffic jam bandwidth field, the data packet is feedback to the source. In resource reservation technique, if the available bandwidth is greater than traffic jam bandwidth. Using rate monitoring and adjustment methodologies, rate control is performed for the overcrowded flows.

To achieve content unobservability, anonymity, unlinkability an PPRP [3] is proposed by employing anonymous key establishment based on group signature. The setup of PPRP is simple: each node only has to obtain a group signature signing key and an ID-based private key. The unobservable routing protocol is then executed in two phases. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination.

II. RELATED WORK

Trust relationships in MANETs are established, evolved, propagated and expired or terminated on fly (no infrastructure). In other words, there is no a priori

trusted subset of nodes to support the network functionality. And Trust may only developed over time, while trust relationships among nodes may also range.

Pirzada and McDonald introduced the notation of belief in their communication trust based model in [4], which provides a dynamic measure of reliability and trustworthiness suitable for applications in an ad-hoc network. Trust model in an adaptation of Marsh's [5] trust model, but they merged utility and importance in one variable called weight for simplicity. They categorized trust into different categories and calculated trust as a sum of all these weighted categories. Based on the protocol and on the scenario to which the trust model is applied, the total number of categorized with trust was defined. The main goal of their model was to build route trustworthiness in nodes by extending the dynamic source protocol to receive a complete list of all nodes through which a protocol has passed.

R.Gunasekaran [6] proposed the high-privileged and low-privileged architecture (HPLP) for Ad Hoc network for achieving optimal differentiated services for different classes of users. The new protocol, DMACAW, was implemented.

ASR [7], ARM [8], AnonDSR [9] and ARMR [10], also make use of one-time public/private key pairs to achieve anonymity and unlinkability. ASR is designed to achieve stronger location privacy than ANODR [11], which ensures nodes on route have no information on their distance to the source/destination node. As the routing onion used in ANODR exposes distance information to intermediate nodes. ARM considered to reduce computation burden on one-time public/private key pair generation. Different from the above schemes, ARMR uses one-time public keys and bloom filter to establish multiple routes for MANETs. An SDAR and ODAR [12] use long-term public/private key pairs at each node for anonymous communication. These schemes are more scalable to network size, but require more computation effort. For example, SDAR is similar to ARM except ARM uses shared secrets between source and destination for verification. Unfortunately, ODAR provides only identity anonymity but not unlinkability for MANET, since the entire RREQ/RREP packets are not protected with session keys. An ALARM [13] makes use of group signature to preserve privacy. The group signature has a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaks lot sensitive privacy information: network topology, location of every node.

III. PROPOSED WORK

1. PERCENTAGE BASED TRUST MANAGEMENT SYSTEM

In this approach, the trust level in a node is defined as a cumulative value that is based on percentage based computation. It takes 60 % of Beacons and 40% of Acknowledgements.

$$TV = 0.6 * bcn + 0.4 * ack. \quad (1)$$

By evaluating the above formula the trust is calculated in all nodes by communicating with one hop neighbor node and the entire topology is referred as community.

A. Community and Community Key Management

In our system, a node's community is as the set of nodes that includes the node itself, referred as central node, and all of its one-hop neighboring nodes, among which some may be malicious. In this approach, the central node classifies its neighboring nodes into three classes, based on their trust level. The first and lowest trust level is for nodes whose trust value is between 0 and 1, while the second trust level, i.e. the medium level, contains the nodes whose trust level is between 1 and 2. The trust level, corresponding to the high level, contains the nodes whose trust value is between 2 and ∞.

The central node generates two different keys for the medium and high trust level, and shares them with its neighbors. All neighbors in the same trust level share the same key. The neighbors in high trust level will have both High Trust Level Community Key (HTLCK) and Medium Trust Level Community Key (MTLCK), whereas, the neighbors in medium trust level have only MTLCK. As for the neighbors in low trust level, they do not share any community key at all. When the central node detects a new neighbor, it will assign an initial trust value to it and updates this trust level later on, based on their interaction.

B. Trustworthy intermediate node selection mechanism

When a source node initiates the Trust establishment process, it specifies the trust level requirement in the initial message. Each intermediate node will propagate the message only to selected neighboring nodes, depending on the source node requested trust level. If the requested trust level is high, the node will use the community key for the neighbors

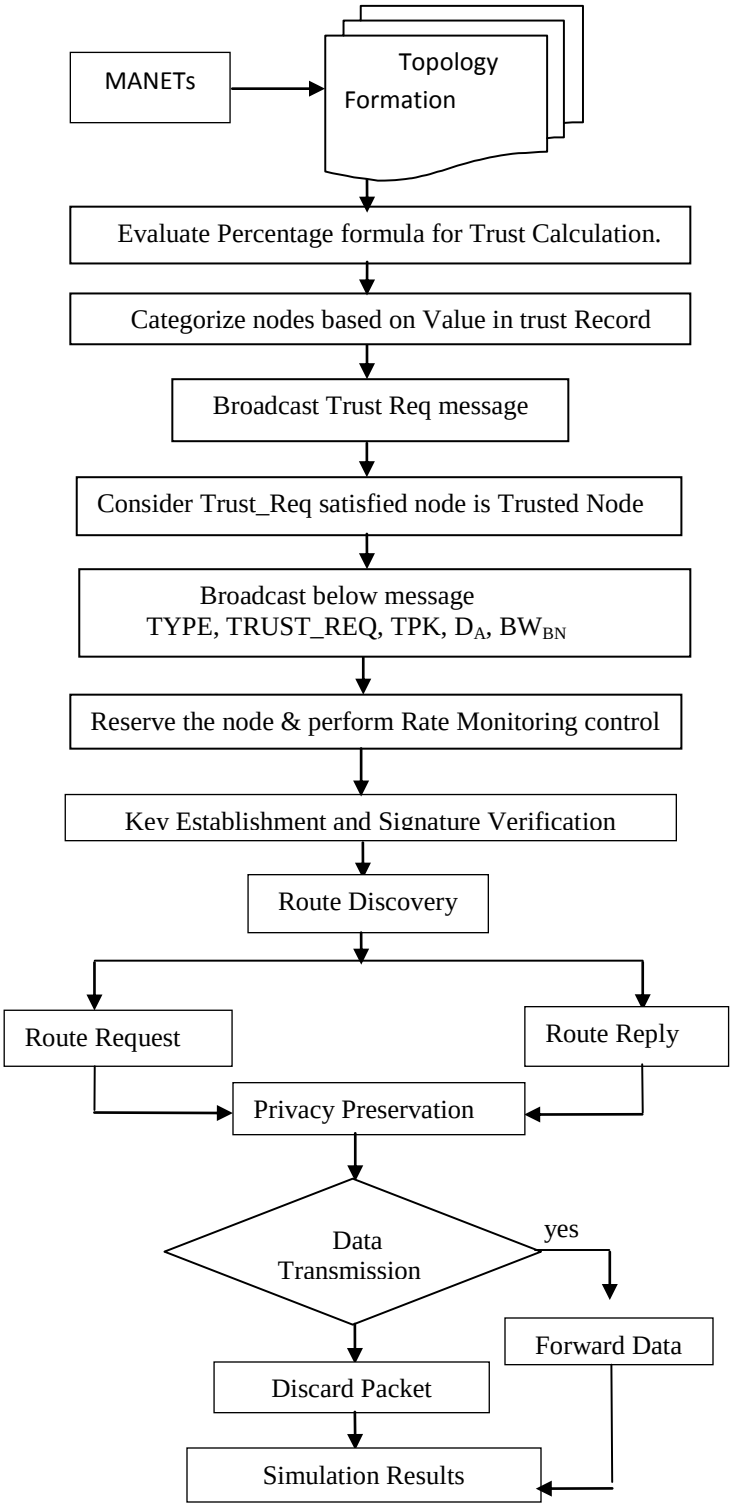


Figure 1: Overall Process Diagram

with high trust level to encrypt the message this will ensure that only highly trusted nodes will participate in the node selection. If the required trust level is medium, the node will use the community key for the neighbors with medium or high trust level to encrypt the message. Using this approach restricts the participation of intermediate nodes only to the ones that have a certain trust level. The source node S triggers the trust establishment phase by sending a trust establishment message to all nodes within its range. It consists of message type (TYPE) trust requirement (TRUST_REQ) and a one-time public key (TPK). The trust requirement indicated by TRUST_REQ could be HIGH, MEDIUM or LOW. TPK is generated for each message and used by each intermediate node to encrypt routing information appended to the message. This key serves also as a unique identifier for the message. The source node prepares and broadcast the following message to all its neighbors.

TYPE, TRUST_REQ, TPK (2)

The trust establishment message is forwarded from one node to other in the network until it reaches the all nodes in topology. When the intended intermediate node gets the trust establishment message it checks the message was received previously, if yes drop it silently and stop. If node is intended node it send reply message to source node to indicate its willingness to become trusted node and accepts the trust requirement in request message. The below figure shows trust management system.

2. BANDWIDTH RESERVATION TECHNIQUE

The source starts forwarding the data packets through the trusted intermediate nodes which containing minimum cost, congestion and bandwidth availability path.

A .Steps involved in Resource reservation

Step1

The source node forwards the data packet that contains the TRUST-REQ, address of source and destination, flow ID and requested data rate stored in the BW_{BN} field to the destination. The source node prepares and broadcast the following message to all its neighbors.

TYPE, TRUST_REQ, TPK, D_A, BW_{BN} (3)

Step 2

The intermediate node upon receiving the data packets determines the B_{av} on its outgoing link.

Step 3

If B_{av} is greater than the BW_{BN} (bottleneck bandwidth) value, then Node forwards the packet to the next node on the path

Else

Node replaces the BW_{BN} field with the value of B_{av} and forwards the packet to next node.

End if

This process continues till packet reaches the destination.

Step 4

When the destination node receives the packet, it copies the value of the BW_{BN} to the new packet and sent back to the source node using the reverse path.

Step 5

The intermediate node upon receiving the data packet updates its routing table with the new BW_{BN} and then forwarded the packet to the next node.

Step 6

When the data packet reaches the source node, the source establishes the real-time flow based on the value of the BW_{BN} field. If the value of B_{av} in source node is greater than or equal to the BW_{BN} value in the packet. Then reservation of bandwidth for the flow can proceed

Else

The BW_{BN} value in the new data packet is overwritten with the (smaller) value B_{av}.

end if

B . Rate monitoring

In the rate monitoring strategy for a real time flow, the rate of flow is measured and compared with the assigned rate which is updated in the routing table. If the rate measured is lesser than the reserved rate by the sufficient margins, then the reserved rate is reduced by certain factor. The below figure shows Resource reservation system.

3. PPRP: Privacy Preserving Routing Protocol

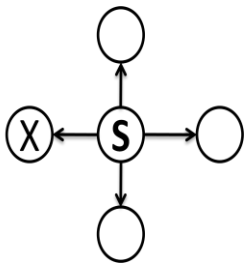
The Privacy Preserving Routing Protocol comprises of two phases: anonymous key establishment as the first phase and the route discovery process as the second phase. In the first phase of the scheme, trusted bandwidth reserved node employs anonymous key establishment to anonymously construct a set of session keys with each of its trusted neighbors. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node. The below diagram shows anonymous routing scheme.

A. Anonymous key establishment

(1) Group signature is computed using its private signing key, other nodes can verify this signature using the group public key. Then it broadcasted within its trusted neighborhood.

(2) A trusted neighbor *X* of *S* receives the message from *Source S* and verifies the signature in that message. If the verification is successful, *X* chooses a random number and computes a signature using its own private key.

(3) Upon receiving the reply from *X*, *S* verifies if it is valid, *S* proceeds to compute the session key between *X* and itself. *S* also generates a local broadcast key K_S*, to its neighbor *X* to inform *X* about the established local broadcast key. Then *X* receives the message from *S* and computes the same session key. It then decrypts the message to get the local broadcast key K_S*.



1. S → *: Trust_Req, $BW_{BN,}$ r_sP, $SIGg_{skS}$ (r_SP)

2. X→S: r_xP, $SIGg_{skx}$ (r_xP), $E_{ksx}(K_s*)$

3. S→X:$E_{ksx}(K_s*)$

Figure 2. Anonymous Key establishment

Figure 2 illustrates the anonymous key establishment process. Below table shows notations used in proposed system.

Table I: Notations

HTLCK	High trust Level Community Key
MTLCK	High trust Level Community Key
TYPE	Message Type
TRUST_REQ	Trust Requirement
TPK	Temporary Public Key
BW_{BN}	Bottleneck Bandwidth
Av	Available Bandwidth
A	A node in Ad hoc N\W, and its identity
S	Secret key owned by server
gsk_A	Node A's private group signature key
gpk	The public group signature key
K_A	Node A's private ID based key
$E_A(*)$	ID based encryption using A's public key
K_{A*}	A local broadcast key
K_{AX}	Session key shared b/w A and X
Nym_A	Pseudonym only valid within A's neighborhood
Nym_{AX}	Pseudonym shared between A and X

B. Route Request (RREQ):

S chooses a random number, and uses the identity of node *D* to encrypt a trapdoor information that only can be opened with *D*'s private IDbased key, *S* then selects a sequence number for this request, and another random number as the route pseudonym, which is used as the index to a specific route entry. To achieve unobservability, *S* chooses a nonce and calculates a pseudonym . After that, *S* encrypts these items using its local broadcast key K_{S*}. Finally, *S* broadcast the below request:

$Nonce_S$, Nym_S, $E_{kS*}(RREQ, N_S, E_D(S, D, r_SP), seqno)$ (4)

Upon receiving the request message from *S*, *A* tries all his session keys shared with all neighbors to calculate $H3(K_{X*}|Nonce_S)$ to see which one matches the received Nym_S. Then *A* would find out k_{S*} satisfies $Nym_S = H3(K_{S*}|Nonce_S)$, so he uses k_{S*} to decrypt the ciphertext. After finding out this is a route request packet, *A* tries to decrypt E_D using his private IDbased key to see whether he is the destination node. Suppose, *A* is not the destination and his trial fails, so he acts as an intermediate node. *A* generates a nonce and a new route pseudonym for this route. He then calculates a pseudonym. At the end, *A* prepares and broadcast the below message:

$Nonce_A$, Nym_A, $E_{kA*}(RREQ, N_A, E_D(S, D, r_SP), seqno)$ (5)

Other node does same as *A* does. Finally, the destination *D* receives the following message from C

$Nonce_c$, Nym_c, $E_{kc*}(RREQ, N_c, E_D(S, D, r_SP), seqno)$. (6)

Likewise, *D* finds out the correct key K_C* according to the equation $Nym_C = H3(k_C*|Nonce_C)$. After decrypting the ciphertext using k_C*, *D* records route pseudonyms and the sequence number into his route table. Then *D* successfully decrypts E_D to find out he is the destination node.

C. Route Reply (RREP):

The destination *D* chooses a random number and computes a cipher text showing that he is the valid destination capable of opening the trapdoor information he sends the below message to *C*:

$Nonce_D$, Nym_{CD}, $E_{kCD}(RREP, N_C, E_S(D, S, r_SP, r_DP), seqno)$. (7)

When *C* receives the above message from *D*, he identifies who the sender of the message is by evaluating the equation $Nym_{CD} = H3(k_{CD}|Nonce_D)$. So he uses the right key k_{CD} to decrypts the ciphertext, then he finds out which route this RREP is related to according to the route pseudonym N_C and *seqno*. *C* then searches his route table and modifies the temporary entry at the end, *C* chooses a nonce $Nonce_C$, computes $Nym_{BC} = H3(k_{BC}|Nonce_C)$, and sends the following message to *B*:

$Nonce_c$, Nym_{bc}, $E_{kbc}(RREP, N_b, E_S(D, S, r_SP, r_DP), seqno)$ (8)

Other nodes perform the same operations as *C* does. Finally, the following route reply is sent back to the source node *S* by *A*

$Nonce_A$, Nym_{SA}, $E_{KSA}(RREP, N_S, E_S(D, S, r_SP, r_DP), seqno)$. (9)

S decrypts the cipher text using the right key *kSA* and verifies that $E_S(D, S, r_SP, r_DP)$ is composed faultlessly.

D. Unobservable data transmission

The packets from *S* must traverse *A*, *B*, and *C* to reach *D*. The data packets sent by *S* take the following format

$Nonce_S$, Nym_{SA}, $E_{kSA}(DATA, N_S, seqno, E_{kSD}(payload))$. (10)

Upon receiving the above message from *S*, A composes and forwards the following packet to *B*:

$Nonce_A$, Nym_{AB}, $E_{kAB}(DATA, N_A, seqno, E_{kSD}(payload))$. (11)

The data packet is forwarded by until it reaches the destination node *D*. At the end, the following data packet is received by *D*:

$Nonce_C$, Nym_{CD}, $E_{kCD}(DATA, N_C, seqno, E_{kSD}(payload))$. (12)

IV. SECURITY ANALYSIS

A. Proposed system is able to establish a certain trust requirement if no of Untrusted nodes available in topology

During the trust establishment process, a source node broadcasts the trust requirement message to all of its neighboring nodes, suppose if any node satisfies the trust requirement in message then the satisfied node will become trusted intermediate node in topology for particular source node. The nodes not satisfying the trust value in message is not considered for communication so the malicious nodes are prohibited.

B. Effective utilization of available resources

This technique enables the source node to select a path to destination which has minimum cost, congestion control, bandwidth and this will be take place through trusted intermediate nodes from source to destination. Suppose if trusted node is not containing required bandwidth for transmission that node will node considered and will dropped, here the nodes having required bandwidth will be considered. This technique avoids transmission of packets to all trusted nodes only the nodes containing the required bandwidth specified by source node will take place in transmission process.

C. Anonymity

User anonymity is implemented by group signature which can be verified without disclosing one's identity. Group signature is used to establish session keys between neighboring nodes, so that they can authenticate each other anonymously. And subsequent routing discovery procedure is built on top of these session keys. Hence it is easy to see that PPRP fulfills the anonymity requirement under both passive and active attacks, as long as the group signature is secure.

D. Unlinkability

The trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key.

E. Unobservability

A node and its next-hop node or previous-hop node on route establish a session key anonymously, hence no one is able to know real identities of its next-hop node or previous-hop node. Even the source and the destination node do not know real identities of the intermediate nodes on route. As a result, PPRP offers content unobservability for ad hoc networks.

V. SIMULATION RESULTS

The Proposed system performance is evaluated in terms of Packet delivery ratio, Throughput and Packet drop. With Figure 3 the proposed system has the higher packet delivery ratio for both types of traffic loads. The reasons are

1) In proposed system only trusted neighbors will forward packets, otherwise packets are simply dropped.

2) Only the nodes containing Sufficient bandwidth has packet forward facility.

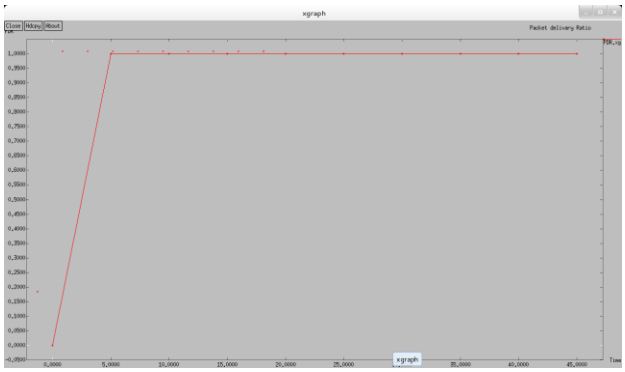


Figure 3. Packet delivery ratio

With Figure 4 the proposed system has high Throughput when comparing with AODV. The average speed of successful message delivery over a communication channel is higher than AODV.

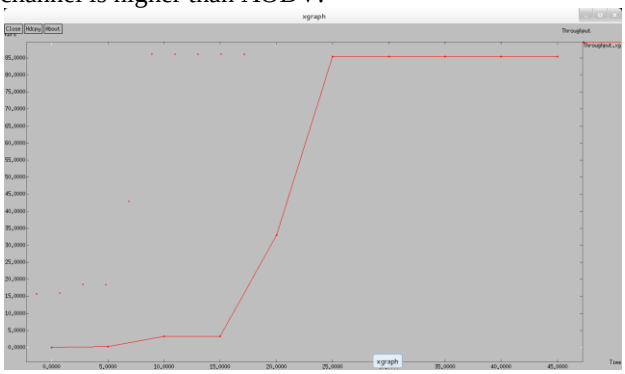


Figure 4. Throughput

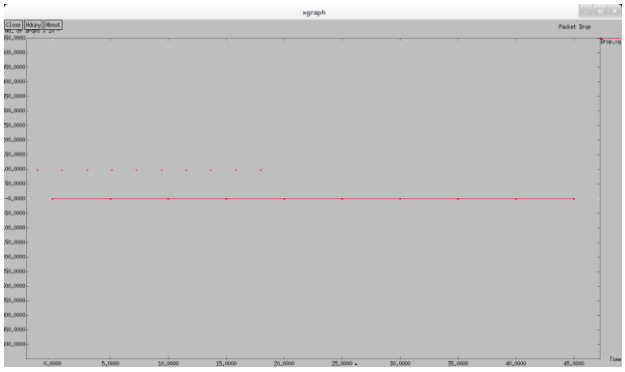


Figure 5. Packet drop ratio

With Figure 5 the proposed system has excellent packet drop ratio. The packet drop ratio will be Zero because of following reasons

1. Intermediate nodes are trusted.

2. Anonymous keys are established with other nodes.
3. Nonce's and Route Pseudonyms are used in route Discovery.
4. Unobservable Data transmission will take place based on Route Pseudonymous

VI. CONCLUSION

In this paper, we have proposed an Percentage based Trust Model with Bandwidth Reservation technique for privacy preserving routing in MANETs. Percentage based Trust management system is proposed to allow trustworthy intermediate nodes to participate in path construction with resource reservation technique to allow trusted nodes to select a path which has minimum cost, congestion and bandwidth. Then PPRP is proposed to offer complete anonymity, unlinkability and unobservabilty for all types of packets. The proposed system offers strong privacy protection, complete anonymity, unlinkability and content unobservability for ad hoc networks. The proposed scheme is implemented in ns2 and examined performance, which shows that proposed protocol has satisfactory performance in terms of packet delivery ratio, Throughput and Packet drop. Future work along this direction is to study how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

REFERENCES

[1]. S Azzedine Boukerchea.B, Khalil El-Khatiba, Li Xu "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks", IEEE Trans.Mobile Comput., vol.1, no.1, Mar. 2002.
[2]. Sarita Singh Bhadauria and Vishnu Kumar Sharma Department of Elex, MITS, "India Bandwidth Reservation Routing Technique Based on Agent in MANETs Using Rate Control with AODV".
[3]. Zhiguo, Kui Ren, and Ming Gu " USOR: An Unobservable Secure On-Demand Routing Protocol for MANETs", IEEE Transactions on wireless communications, May 2012.
[4]. A.A. Pirzada and C. McDonald, "Establishing Trust in pure Adhoc Networks", in the 27th Australasiam Conference on Computer Science, Dunedin, new Zealand, 2004.
[5]. S. Marsh, "Formalising Trust as a Computational Concept", in Department of CS and mathematics, Vol. Phd:university of Stirling,1994,pp. 184.
[6]. R. Gunasekaran and V. Rhymend Uthariaraj, "Differentiated Bandwidth Allocation in MANET – A Profile Based Approach", Asian Journal of IT
[7]. K. E. Defrawy and G. Tsudik,"ALARM: anonymous location-aided routing in suspicious MANETs", IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1358, 2011.
[8].S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks", in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications
[9]. J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks", in Proc. ACM MOBIHOC' 03.
[10]. Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks", Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.
[11]. J. Kong and X. Hong, "ANODR: anonymous on demand routing with untraceable routes for MANETs.
[12].D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks", in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.
[13].K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs", IEEE Trans. Mobile Comput., vol. 10,no. 9, pp. 1345–1358, 2011.

BIOGRAPHY

1. **Mr. R. Raghu**[1] obtained his bachelor's degree in Information Technology from Adhiyamaan college of Engineering affiliated to Anna University, Chennai. Currently he is pursuing his Master degree in CSE at Adhiyamaan College of Engineering, Hosur, Tamilnadu.

2. **Prof. B. Gopinathan**[2] obtained his bachelor's degree in Information Technology from M.I.E.T Engineering College, Trichy-7. And He received his Master degree in CSE from Arunai Engineering College, Tiruvannamalai. Currently he is pursuing his Ph.D at Anna University, Chennai, in the field of Ad hoc networks.. He has 6 years of teaching experience and currently, he is working as a Associate Professor in CSE Department at Adhiyamaan college of Engineering, Hosur, Tamilnadu.