AN UNOBSERVABLE PRIVACY PERSERVING TIK PROTOCOL IN MOBILE AD HOC NETWORKS

L.Aswathy Lal*

J.Nalini**

Abstract

Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. Providing privacy protection with low-power wireless devices and low-bandwidth network connection is difficult task.Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. Existing schemes can not protect all contents of packet from attackers so that the attacker can obtain information like packet type and sequence number etc..Most of the privacy perserving routing protocols contains anonymity and unlinkability.USOR is the first unobservable routing protocol.This protocol doesn't prevents wormhole attacks and denial of service attack.So the modified system use a protocol which is to be prevent against wormhole attack.An efficient authentication protocol TIK is to be used with the help of temporal leashes. This protocol supports the symmetric key cryptosystems. It removes out all attackers and complete protection of packet occurs through the protocol.

***Keywords*— Unobservability, Unlinkability, Routing protocols, security, anonymity, privacy.**

* P.G Student, Department of Electronics And Communication, PSN college of Engineering and Technology, Tirunelveli

** Assistant Professor, Department of Electronics And Communication , PSN college of Engineering and Technology, Tirunelveli

I. INTRODUCTION

Secured communication has wide range of applications. In wired networks has certain disadvantages compared to wireless communications.Wireless communication needs privacy protection. Secured communication is used in military communication and national security.Without privacy protection data cannot be transmitted.Privacy protection is more important in wireless networks.Wired communication uses cables for the connection so privacy protection is not needed for the communication.In wireless communication is easily affected by the attackers.Because it cannot uses connection wires.MANET is the infrastructure less network.So the protection of data is more important in MANET.Attacker needs an appropriate transceiver to receive the wireless signal.Wired networks is difficult to move from one place to other.So wired network does not need to protect users mobility,path and sensitive information should be kept as private.Otherwise the attackers should hack or attack the packets or information based on the information which is to be leak out. A low bandwidth network connection and low power wireless device in ad hoc is risky.

Unobservability, unlinkability and anonymity terminologies are very important in privacy protection of ad hoc networks .For privacy protection many routing schemes are to be used.These existing routing schemes only consider anonymity and partial unlinkability in MANET.Most of the protocols mainly used to achieve privacy by using asymmetric feature of public key cryptosystems. Unobservability and unlinkability are to be completely provided for proper protection.Most of the existing schemes fail to protect the packets from attackers because of easily getting the information like packet type and sequence number etc.These types of information will leaks or breaks the unlinkability and may lead to source trace back attack,wormhole attacks and denial of service attacks.So these types of information can be kept secret to achieve the complete unlinkability,unobservability and anonymity.

Unobservability property of the packet is to be done as soon as possible to obtain the security.Unlinkability property is not enough in the hostile environments.Passive attacker or indirect attacker only monitors unencrypted traffic and looks for clear text passwords and sensitive information that can be used in other types of attacks.For protection the information on packet type and node identity like to be kept as secret.Careful design is to be used to be remove the linkability by using decryption and encryption techniques.The demerits of the existing

schemes is that they use public key cryptography and which leads very high computational overhead.

Unobservability is the strongest criteria.To achieve the unobservability property is to be difficult and the corresponding routing scheme should provide unobservability for both content and traffic pattern.In content unobservability no useful information is extracted from the content of the message and traffic pattern unobservability no useful information can be obtained from the frequency,length and source to destination patterns of the message traffic.Content unobservability is to be used in this paper.Traffic unobservability only used to achieve truly unobservable communication MIXes and padding is to be used to achieve protection.

In this paper we propose an unobservable privacy preserving routing protocol UPPR that achieves content unobservability by anonymous key establishment.Contribution of this paper include 1)Implementation of UPPR on ns2 2)Detailed security analysis and comparison between USOR and other related protocols.Appropriate traffic padding schemes is to be used to protect the communication. The rest of this paper is arranged as follows.In the next section; we discuss related work on anonymous routing schemes for adhoc networks.Routing scheme in section II. Finally, we summarize and conclude the paper.

II. RELATED WORK

For to achieve privacy protection in MANET a number of routing schemes are to be used.It uses different cost for different levels of privacy protection.Most of the routing schemes uses public key cryptosystems to achieve anonymity and unlinkability.PKC operations have high computational overhead assymetric PKC is better for privacy protection.

ANODR scheme proposed by Kong is the first one to provide anonymity and unlinkability for routing in ad hoc networks.It uses PKC based schemes.For route discovery process onion routing is to be used.Anonymity and unlinkability property is mainly considered by ANODR for this it uses one time public/private key pair for encryption and decryption.For this scheme packets are publically labelled and the attacker is easily distinguish the packet,so the scheme fail to guarantee the unobservability property.

One time public/private key pairs are to be used by the schemes are ASR,ARM,AnonDSR,ARMR etc.ANODR is less efficient than that of ASR.Onion routing exposes distance information to intermediate nodes, which causes the demerits of the

system.ASR cannot use onion routing.In ANODR packets are publically labelled and the attacker is able to distinguish different packet types,which fails to guarantee unobservability.ASR provides privacy and security and it provides additional properties anonymity.In AnonDSR one time PKC is used and sender and receiver anonymity occurs in it.ARMR uses bloom filter to establish multiple routes,ARM use time to live mechanism and padding techniques.It is less efficient.

SDAR and ODAR uses long term public/private key pairs for anonymous communication.SDAR is similar to ARM except ARM uses shared secrets for verification.ODAR cannot provide unlinkability for MANET.In this RREQ/RREP packets are not protected with session keys .In AODV tunnelling can be done on the basis of route request(RREQ) and route reply(RREP) packets. If RREQ packet is directly send to the destination, when the destination nodes neighbours hear the request, they will follow the routing protocol for processing to rebroadcast the copy of request and discard without processing all other route request packets.The original packet will found out the route. This type of route discovery will avoid the nearest attackers. This discarding nature will certain times causes denial of service attacks.

PUZZLE is based on scalable secret sharing.It also provides high degree of anonymity.High degree of anonymity and reliable message delivery are to be provided by using this protocol.The disadvantages is mainly caused by shared flooding and it has low security overhead.In rumer riding uses non path based routing schemes and uses symmetric cryptosystems.

An anonymous location aided routing in MANET, ALARM uses public key cryptography and uses group signature.Group signature has high privacy preserving feature that is everyone can verify the signature but the signer only can identify it.But this protocol leaks out sensitive informations.

To summarize, public key cryptography have preferable asymmetric feature and is mostly used for privacy protecttion in MANET.Privacy protection is the main task for public key cryptosystem. It is the second unobservable routing protocol.Drawback of the existing scheme is the existing scheme is that packets are affected by the wormhole and denial of service attacks.Delay is to be high in the existing routing schemes.

III. DETECTING WORMHOLE ATTACK

In wireless communication there are two methods which are to be used to detecting the wormhole attack.They are an efficient authentication protocol TIK using temporal leashes and topology based wormhole detection.The second method cannot determine all types of wormhole attacks.So we use efficient authentication protocol TIK using temporal leashes are to be used.We assume that the nodes can be places anywhere in the network, that is, the nodes are connected through a channel that is unobservable by other nodes.For the wormhole detection we use efficient symmetric key cryptography.In CPU limited devices symmetric cryptographic operations are three to four order of magnitude faster than assymetric cryptographic systems.TIK uses only symmetric cryptography traditional public key system for key distribution is to be created.The corresponding public key system generated a trusted entity which can sign public key certificates for each node and then use their public key to sign a new (symmetric) key being distributed for use in TIK.

Wormhole Attack

Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and this is the reason the attacks are serious. In wormhole attacks the attacker records packets received at one location in the network and tunnel them to another location and retransmits them into the network.An approach to detect the wormhole attack is based on the packet leashes. The main intuition uses the main intuition is that by authenticating either an extremely precise timestamp that is temporal leashes or location information combined with a loose timestamp that is geographical leashes ,a receiver can determine if the packet has traversed a distance that is unrealistic for specific network technology used. We can use 4 steps to explain about a general wormhole attack.

1. An attacker has two trusted nodes (or two colluded attackers each has one node) in two different locations of a network with a direct link between the two nodes.
2. The attacker records packets at one location of a network.
3. The attacker then tunnels the recorded packets to a different location.
4. The attacker re-transmits those packets back into the network location from step 1.

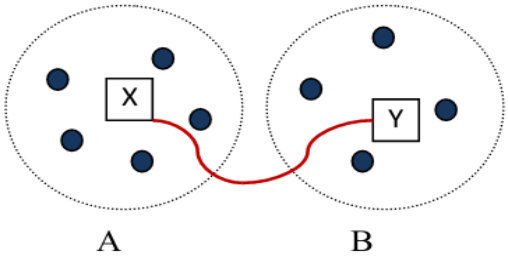


Fig. 1 Example of wormhole attack

Denial of Service Attack

The network resource is unavailable to its intended users.The efforts of one or more people to temporarily or indefinitely interrupt or suspended services of a host connected to the internet.This attack is the serious attack for the whole network.It causes complete disruption of the routing function and the whole operation of mobile ad hoc network.Depending upon the context of anonymous routing denial of service attack can be classified into two types.They are multiple to one attack and one to multiple attack.

During the packet design leashes is used to restrict the packets maximum allowed transmission distance.For a single transmission leashes are used to protect against the wormhole attack.When multiple transmission occurs then each transmission requires a new leash.A geographical leash ensures that the receipient of the packet is within a certain distance from the sender and the temporal leash ensures that the packet has an upper bound on its lifetime, and it restricts the maximum travel distance.

A. Temporal Leashes

To construct a temporal leash , all nodes must have tightly synchronized clocks, maximum difference between any two node clock is Ω.The corresponding values is known to all nodes in the network and the value of Ω be on the order of a few microseconds or even of nanoseconds.Defend against wormhole attack requires time synchronization.In temporal leashes, the node sending the packet time be Ts and the node receiving the packet time be Tr.The

corresponding receiver can identify variation in transmission time by comparing Tr and Ts then by identifying that the packet is travelled too far or not.

B. Implementation Details

Temporal leashes are implemented with a packet expiration time.Consider a sender who want to transmit a packet with a temporal leash which would prevent the packets from travelling further than distance l.Then l > lmin = Ω.S,where S is the speed of wireless signal.Then the packet expiration time is calculated Te= Ts + l/s - Ω.Then the receiver checks Tr < Te.Otherwise it drops the packets.The receiver must authenticate the expiration time otherwise the attacker can change that time and wormhole attack occurs.

In TIK an efficient hash tree is used for the authentication mechanism.The hash tree consists of sequence of values u0,u1,…uv-1.and we place these values at the leaf nodes of a binary tree.Then we consider a one way hash function .So ui'=H(ui)for each i.We then use the Merkle hash tree construction to commit to the values u0,u1,…,uv-1.here each internal node of the binary tree is derived from its two child nodes.

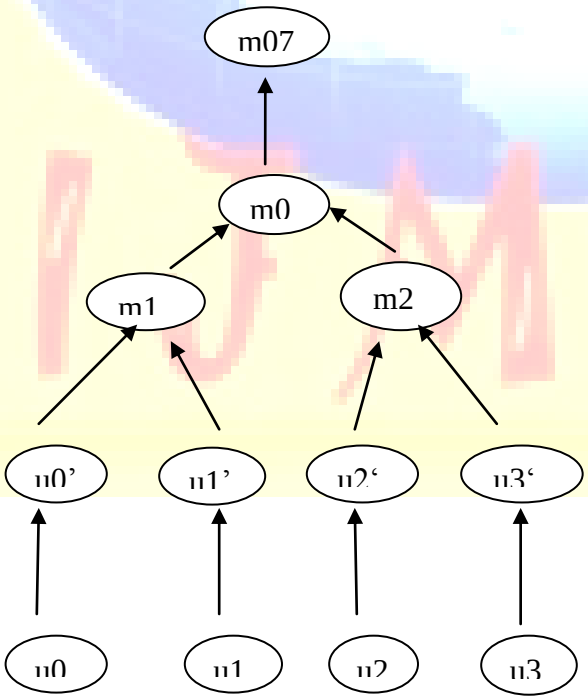
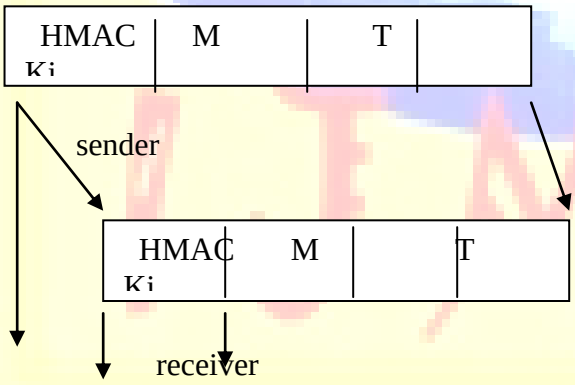


Fig 2. Merkle hash tree

C. TIK Protocol

TIK protocol provides efficient instant authentication for communication.TIK means TESLA with instant key disclosure.In TIK packet transmission time can be significantly longer than the synchronization error.Then the receiver can verify the TESLA security condition.An efficient broadcast hash tree autentication is provided for the TIK protocol.TIK uses a temporal leash and which enables the receiver to detect the wormhole attack.It uses an efficient symmetric cryptographic primitives. In this the sender and the receiver uses the same keys. It requires accurate time synchronization between the communicating parties. Scalable secret key distribution occurs through the corresponding nodes.TIK protocol consists of different stages: sender set up, receiver bootstrapping and sending and verifying authenticated packets. It provides protection against wormhole attack, the attacker who retransmits the packet which will most likely to delay its long and it will reject the packet because the corresponding key is expired.



Ts ≤(Ts+μ+Ω) ≤(Ti-Ω)

Fig 3.Packet timing using TIK

D. System Setup

Consider an ad hoc network consisting of n nodes with the same communication range and each and every node can move around within the network.The traffic analysis is prevent based

on the MAC addresses.One node can communicate with other nodes by direct path (single hop) or multihop path.

E. Attack Model

A global adversary model is developed which is to be capable of monitoring developed which is to be capable of monitoring traffic of the entire ad hoc network.The corresponding model can monitor and record all types of information in the network and analyse the result using the source and destination packet.Then the active,passive and wormhole attacks are to be lunched to attract the network traffic.Then the attacker should breakdown the privacy factors like anonymity,unlinkability and unobservability.An efficient protocol TIK is used to remove out the wormhole attack.It is to be based on the symmetric key based system.

Assume that the pseudorandom function PRF is secure ,which is computationally difficult for the attacker to derive a key ϵ.For to construct the PRF function F, we can use a pseudorandom permutations like block cipher or a message authentication code (HMAC).The sender selects a key expiration interval,I which determines the schedule which depends upon the key.Like K0 expires at time T0, key K1 expires at time T1=T0+I and Ki expires at time Ti=T(i-1)+I.Maximum clock synchronization time Ω.When the sender sends a message or packet it estimates the upper bound Tr on the arrival time of HMAC at the receiver.Based on the arrival time sender key Ki will not be expired and when the receiver receives the packet HMAC (Ti>Tr+Ω).Ki key is used to compute the authentication.If packet authentication verifies correctly once the receiver receives the authentic key Ki.The sender and the receiver timelines differ by certain values by the maximum time synchronization error Ω.The sender S begins the transmission and the corresponding TIK packet transmitted by S as

S→R: <HMA Cki(M),M,T,Ki>

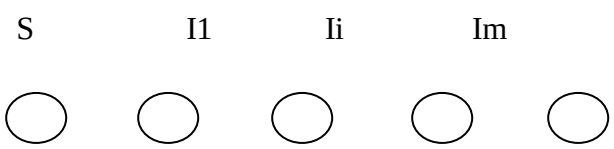


Fig 4. The route of source to receiver

The corresponding destination should be unicast or broadcast.Then the receiver should receives the HMAC values and verifies the key Ki based on time Ti and synchronized clock Ω.If the delay is long then the retransmission of packet occurs.If delay occurs then the corresponding packet is to e removed out.For the temporal leash use an expiration time stamp.

F. Discussion

USOR is the first unobservable routing protocol.It establishes key's between the neighbouring nodes to achieve protection.It uses two schemes that is,onion encryption and end to end security.The previously existing protocols only consider the linkability.USOR does not leaks out the private informations.MASK uses one time pairing based keys for encryption and unobservable routing schemes makes group signatures.Trusted party will generate the one time key.RREQ and RREP signals are used in the routing procedure.Nonce are to be used for each transmission.The nonce are used at a time and never reused, so they are also called pseudonyms.Nearest nodes are to be compromised then the privacy can be protected.Using per hop protection of packets, nodes are to be compromised , which will offer satisfactory protection between the nodes.During the RREP message or data packets which is to be transmitted or send through the compromised node becomes the intermediate node then the corresponding source or destination node cannot be identified by the attacker.

G. TIK Performance

To evaluate the TIK in ad hoc network we measured computational power and memory which are to be currently available in mobile devices. Repeated hashes are to be computed per second and optimized MD5 hash code to achieve better performance. Optimized version performs 10 million hash function evaluations in 7.544 s on a Pentium III running at 1 GHz and the same number of hashes are to be used in this implementation on a Compaq iPAQ 3870 and Pocket PC running Linux took 45 s.Memory consumption of the existing handheld devices such as iPAQ 3870,come equipped with 32 MB of the Flash memory and 64MB of RAM.In sensor networks nodes may be able to achieve time synchronization in 20m range and 19.6kb/s link speed to be achieved.TIK is not usable in resource scarce system. This level of time synchronization in the system, TIK could not provided usable wormhole detection system.

Packet leashes provides the sender and the receiver to ensure that a wormhole attacker is not causing the specified normal transmission range.Geographic leashes are used to detect the tunnelling across devices or obstacles.Malicious receiver can not check the authentication on a packet, which allow the attacker to tunnel a packet to another attacker without trace out and the second attacker, and cannot retransmit the packet until the actual sender without being found out.When the malicious node becomes the sender then it can approach with a false time stamp and causing a legitimate receiver to have mistaken that not the packet was tunnelled. In geographic leashes are used in conjunction with digital signature and the corresponding node to be able to detect malicious node and spread that information to other nodes. The corresponding attacker is equivalent to wormhole attacker and allowing the sender of the wormhole attacker to place appropriate time stamps for the sender or location information of any packet send by the sender that are then to be tunnelled by the wormhole attacker.The compromised node creates a future time stamp into the packet which is to be extended its life time.

Security Based Approach

Many researchers have proposed a method to detect wormhole attack by constructing a model of network topology based on inaccurate distance measurements between the adjacent nodes and decode packets which can choose to tunnel only traffic between two select nodes over a minimum distance , such attacker has minimum effect on the network and it is difficult to detect and analysis. One possible attack is that adversaries send fake route error packet to attack the source and compel to choose another route or even re launch the route discovery process. This makes no sense when adversaries can not route and launch such attack. Therefore these attacks are used on route maintenance only and we consider adversaries which are not present in the corresponding route. There is no shared secret between the consecutive nodes en route and thus a node detecting route failures has difficulties in informing the source failures. Temporal leashes are more efficient. A geographical leash requires a more general broadcast authentication mechanism which increases the computational overhead and network overhead. Network overhead can be increases because of the location information which may require more bits. Geographical leashes have to be used to detect tunnels through obstacles. It does not require the tight time synchronization but the temporal leashes needs it. Geographical leashes are important in certain places where the temporal leashes cannot be applicable. So these two leashes have very

much importance in networks architecture. Preferably we used these techniques to reduce the overhead in the network structure.

IV CONCLUSION

The unobservability is a very important part of the overall solution for securing mobile ad hoc networks. In this paper we first gave an unobservable privacy perserving routing protocol.The unobservable protocol gave a detailed analysis on wormhole attack. For the prevention of wormhole attack we use an efficient authentication protocol TIK based on temporal leashes. This protocol will determine the wormhole attack and it will decrease the bandwidth and increase the packet delivery ratio and security. This type of routing protocol has very importance in ad hoc networks.

REFERENCES

[1] Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity terminologies," July 2000

[2] D. Boneh and H. Shacham, "Group signatures with verifier-local ,"in 2002.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM,1978

[4] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," Dec. 2011

[5] S. Canard and M. Girault, "Implementing group signature schemes with smart cards," in CARDIS'02: Proc. 5th conference on Smart Card Research and Advanced Application Conference Berkeley, CA, USA:USENIX Association, 2002

[6] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. of the ACM, vol. 4, no. 2, Feb. 1981

[7] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput.vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003

[8] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlationattacks and countermeasures in mix networks," in PET04, LNCS 3424,pp.207–225.2004

[9] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM

[10] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.2004

[11] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobilead hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, 2006.

[12] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.2005

[13] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMRN:anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536,2009

[14] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624.2004

[15] 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.2006

[16] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology–Crypto'01,2001

[17] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no.3,pp. 464–475, 2011

[18] J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in Proc. IEEE MASS'09, pp. 332–341.2009

[19] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.2005

[20] 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

[21] "Privacy-preserving location-based on-demand routing in MANETs,"IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 1926– 1934, 2011

[22] J. Han and Y. Liu, "Mutual anonymity for mobile peer-to-peer systems,"IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1009–1019, Aug. 2008.

[23] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in vol.3152, 2004, pp. 41-55.2004

[24] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard:defending against sybil attacks via social networks," in Proc. 2006

[25] I. R. Jeong, J. O. Kwon, and D. H. Lee, "A Diffie-Hellman key exchange protocol without random oracles," in Proc. CANS 2006, vol. LNCS 4301, pp. 37–54.2006

[26] A. Serjantov and G. Danezis, "Towards an information theoretic metricfor anonymity," in Privacy Enhancing Technologies, 2002, pp. 41–53.

[27] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011

[28] M. Scott, "MIRACL: Multiprecision Integer and Rational Arithmetic C/C++ Libra1990

[29] N. Abramson, "The ALOHA system—another alternative for computer communications," in Proc. 1996

[30] Specification sheet for ORiNOCO world PC card, Agere Systems Inc.[Online]. 2000

[31] ARC releases blueForm, a comprehensive solution for bluetooth systems on a chip, ARC International.1998

[32] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in Lecture Notes in Computer Science, N. Koblitz, Ed. Berlin, Germany: Springer-.Advances 2000

[33] B. Bellur and R. G. Ogier, "A reliable, efficient topology broadcast protocol for dynamic networks," in ProcCompu. Commun., Mar. 1999

[34] S. Brands and D. Chaum, "Distance-bounding protocols," in Lecture Notes in Computer Science,Cryptographic Techniques 1996

[35] Tom Clark's totally accurate clock FTP site, T.Clark.Available:ftp://aleph.gsfc.nasa.gov/GPS/totally.accurate.clock/2000

[36] A. K. Lenstra and E. R. Verheul. Selecting Cryptographic Key Sizes. In Public Key Cryptography, pages 446–465, 2000.

[37] M. K. Marina and S. R. Das. Ad Hoc On-demand Multipath Distance Vector sRouting. In ICNP, pages 14–23, 2001.

Author's Profile:

L.Aswathy Lal is doing her ME in Communication Systems at PSN College of Engineering And Technology, Tirunelveli. She received her B.Tech in Electronics And Communication from SHM Engineering College, Kadakkal, Kerala in 2010. Her research interests include wireless communication.

Mrs.J.Nalini is presently working as the assistant professor in PSN College of Engineering And Technology, Tirunelveli. She received her M.Phil in Electronics and ME in Communication systems.