SHARED INFORMATION BASED SECURITY SOLUTION FOR MOBILE AD HOC NETWORKS

Shailender Gupta[1] and Chander Kumar[2]

[1]Department of Electronics Engineering, YMCA Institute of Engineering, Faridabad
shailender81@gmail.com
[2]Department of Computer Engineering, YMCA Institute of Engineering, Faridabad
nagpalckumar@rediffmail.com

ABSTRACT

The mobile ad hoc networks get subjected to security threats like other wireless networks. But due to their peer to peer approach and absence of infrastructural resources the mobile ad hoc networks can not use strong cryptographic mechanisms as used by their other wireless counterparts. This led to the development of trust based methods as security solutions wherein a trusted node is relaxed from security checks when the trust value reaches to a particular limit. The trust methods are prone to security risks but have found their acceptance due to efficiency over computationally expensive and time consuming cryptographic methods. The major problem with the trust methods is the period during which trust is growing and is yet to reach the requisite threshold. This paper proposes security mechanism dependent upon Random Electronic Code Book (RECB) combined with permutation functions. The proposed mechanism has low time complexity, is easier to implement, computationally inexpensive and has very high brute force search value. It can be used as the temporary security guard during the trust growth phase. The impetus behind the proposed design is the reliance upon shared information between the peers in the ad hoc networks.

KEYWORDS

Ad hoc Networks, Security, Trust, Cryptography

1. INTRODUCTION

The term Mobile Ad hoc Networks (MANETs) is used for the ad hoc wireless local area networks (Ad hoc WLAN) by the Internet Engineering Task Force (IETF) wherein the mobile nodes can communicate with each other directly without the requirement of support station [1]. Due to their non dependence on the central communication point they can be quickly installed. MANETs can work either in isolation or as extension to a pre installed wired network [2]. The MANETs can be used in the disaster situations such as earthquakes or hurricanes where infra structure facilities such as power and communication lines have been destroyed. They can also be used in planned military operations or in the battle field [3]. Since, MANETs do not have centralized router that helps them in communication, therefore, each node has to act as a router, transmitter and receiver.

The communication between the various nodes in MANETs, which are not lying within the radio range of each other, is through intermediate nodes. Also the nodes are mobile leading to the change in the topology of the network, making the design of routing protocol a challenging task. Any routing protocol designed for MANETs should ensure the following characteristics [1]: distributed operation, freedom from routing loops, on demand operations, proactive operation, security, inactive period operation and unidirectional link support.

The initial routing protocols such as AODV [4], WRP [5] concentrated on the routing process only and were devoid of security mechanisms. With the time efforts were made to incorporate the security feature in the routing protocols [6, 7, 8]. However it was quickly realized that the security incorporation in MANETs is altogether different aspect than in case of fixed wired and wireless LANs where the installed infrastructure takes the major burden of the security of the network. In case of MANETs security process cannot be allowed to resident at a particular location due to the absence of centralised infrastructure and therefore this burden has to be shared by the participating nodes themselves. This makes the cryptography not a suitable solution in the MANETs scenario as the process is highly computationally expensive and the existence of a central agency is a mandatory requirement for key distribution. This led to the development of trust based methods wherein every node in the network keeps the record of the behaviour of other nodes by using a trust index. This index grows/decrements with the time depending upon the behaviour of the nodes with the passage of time. The trust growth is quite slow and it takes time for the trust index to reach a requisite level. Thus an arrangement is required, in the mean time, to keep the network safe. This paper is an effort in this direction.

This paper has been divided into following sections. Section 2 contains literature survey. Section 3 contains the description of the problem. Section 4 describes the proposed solution. Section 5 contains the conclusion. All this is followed by acknowledgement and references.

2. LITERATURE SURVEY

The ad hoc network is built to provide communication among heterogeneous node in the absence of any fixed infrastructure. Initially the protocols developed such as HSRP [9], DSR [10], ZRP [11] and DSDV [12], were devoid of security features. But with the advancement of technology and the need for securing the data from the attacks, the security features were incorporated in the ad hoc routing protocols. The major aspects to be considered while implementing the security feature in the ad hoc network were as follows:

- Shared broadcast radio channel: The radio channel used for communication in ad hoc network is shared by all the nodes in the network. Data transmission by a node is received by all the nodes with in its radio range. So a malicious node can easily obtain data being transmitted in the network.
- Insecure Operational environment: The ad hoc network is setup mostly in disaster hit areas or in battle field. In battle field the node move in and out of its territory so the nodes are more susceptible to security threats.
- Lack of central authority: In ad hoc environment there is no central authority to monitor the traffic so intermediate security check points cannot be installed.
- Lack of association: The nodes move in and out of the network so a malicious node can easily join the network if there is no proper authentication mechanism.
- Limited resource availability: Resource such as battery power, bandwidth and computational processing are scarce in ad hoc wireless networks. Hence it is difficult to implement complex cryptographic operation for such networks.

All these issues made the design of secured routing protocol for ad hoc network, a challenging task for researchers. Before designing any security protocol the researchers keep the following fundamental requirements in mind.

- Detection of malicious node: The routing protocol must be empowered enough to detect the malicious behaviour by any node in the network.
- Guarantee of correct route discovery: If there exist a path between a source and destination then the routing protocol should be able to trace it and should be able to check the correctness of that route.
- Confidentiality of network topology: If the network topology is disclosed to the malicious node then the malicious node may observe the traffic pattern and in turn may attack the

active points of the network. This will disrupt the routing process so the confidentiality of the network topology is important.
- Stability against attack: The routing protocol must be able to recover to its normal state with in a finite period of time.

Based on the above issues and requirements, several security many protocols have been developed by the researchers. The security protocols for ad hoc network are categorized into two categories: Cryptography Based Protocols and Trust Based Protocols.

2.1. Cryptography Based Protocols

The cryptography based protocols can be classified into two categories: Symmetric Key Based protocols and Asymmetric key based.

2.1.1. Symmetric key

These routing protocols use symmetric key cryptography and hash chains to secure the network. The example protocols in this category are SEAD [13], Ariadne[14], SRP[15]. The designers of these protocols have assumed a central authority who will distribute secret key to encrypt and decrypt the data packets to be exchanged between the nodes of the network. SEAD uses symmetric keys for authentic distribution of the hash chain seed. It incorporates one-way hash chains to provide authentication of routing messages. Ariadne is based on symmetric keys for pair wise key distribution between all nodes, and on hash chains for node authentication and so on. The major issues relating symmetric key based protocols are

- They are more secured in comparison with the asymmetric key but the encryption and decryption overhead to create the cipher text is quite high.
- To apply it successfully and efficiently there is a requirement of central authority for the distribution of key.
- The latency caused by the use of symmetric key may not be tolerable.

2.1.2. Asymmetric key

In this method each node has certified set of keys of all the nodes in the network. To route the traffic from source to destination the source node the source node send the packet signed with its private key. The receiver or intermediate node cryptographically validate the signature and the hash value and sign the content of packets with its private key while forwarding. The data is encrypted using public key and decrypted using the private key. The signature protects the routing information and prevents spoofing and other attacks. The popular protocols in this category are ARAN [16], SAODV [17]. The issues relating to the use of asymmetric key are follows:

- The complexity of public key algorithms is $O(n^3)$[25].
- It requires a trusted central authority for distribution of keys.
- They are more suitable for wired network where normally large bandwidth is available and there is a central authority with good processing capability.
- There is a problem of man in the middle attack and the malicious intermediate nodes can easily harm the network activities.
- The delay involved in the symmetric key protocols for MANETs is quite significant.

To secure the ad hoc network against the selfish and malicious behaviour the secure routing protocol use cryptographic tools to protect the information and also ensure that basic under lying routing protocol (which secures the route) is not disturbed. The securing of the route is mandatory because if the packet doesn’t reach the destination there is no fun of protecting the information. As mentioned earlier, the cryptography based protocols presume the existence of centralized or distributed third party in the network. This assumption is also coupled with the pre configuration of the nodes with encryption keys prior to the joining in the network. Thus to implement the cryptography based protocols it is necessary that the ad hoc network be established in the planned manner. Also their operation has to be managed/ supervised. This is a deviation from the purity of the ad hoc network concept. The use of cryptography restricts the size and mode of application in ad hoc networks as well.

In a pure environment, the existence of central authority and pre-configuration of the nodes can not be assumed. These networks are formed in a spontaneous and self organized manner without the requirement of centralized infra structure or authority. Any wireless node can gain or loose the membership of the network at any time without the need for prior registration. For such an environment, the cryptography is not a possible tool. To secure the network in such a scenario trust based protocols have been proposed. In these protocols the nodes in the network assess the performance of their neighbouring nodes based upon their own experience and sharing of information with other nodes. This leads to the computation of the trust factors which is used to derive the reliability and the sincerity of the node. A sincere node is preferred over an unknown or not so sincere node for making the route.

Keeping the above aspects in view, in [26, 27] the authors have proposed a self organised public key system without the requirement of central agency or initial configuration. The users in the ad hoc wireless network issue certificate to each other on personal acquaintance. A certificate is a binding between a node and its public key. The certificates are stored and distributed by the users themselves and are valid for a specified period of time. Upon the expiry of time the certificated is updated by the user who had issued the certificate. So there is an example of trust creation on the basis of acquaintance and thereby issue of public key. The subsequent subsection describes the security mechanisms based upon the calculation of trust index without the use of cryptography.

2.2 Trust based security mechanism

The trust based security mechanisms have been found to be quite computationally inexpensive as the trust computational overhead is quite small compared to cryptography based solutions. The literature contains a lot of protocols based on trust mechanism. For example Watch Dog and Pathrater mechanism [18] has been designed over DSR protocol. The Watchdog is responsible for detecting selfish nodes and the Pathrater assigns the different rating to the nodes depending upon the feed back received from Watchdog. The CONFIDANT [19] protocol contains a trust manager and a reputation system The trust manager evaluates the reports submitted by the monitor (a kind of watchdog) and issues alarms to the other nodes to warn them against a malicious node. The CORE [20] protocol employs a reputation evaluation mechanism based upon three kinds of reputations: Reputation based upon personnel observation (subjective reputation), Reputation based upon the positive reports received from other nodes (indirect reputation), and the Reputation based upon the behaviour of a node during a specific task (functional reputation). These reputations combine to create an overall reputation index about a particular node which can be recommended for inclusion in the network or for isolation. The other protocols in this category are SORI [21], OCEAN [22].

To derive the trust values the behaviour of the neighbours has to be observed with respect to their packet forward mechanism. This requires that when a node transmits a data or control packet it must bring the receiver into promiscuous mode so that it can overhear whether its immediate node has forwarded the packet or not. If yes, the immediate neighbour is reliable otherwise not. To implement the trust based security mechanism the participating node must support the following features [23],

- promiscuous mode operation
- omni directional transceivers
- comparable transmission and reception range of transceivers

The trust based protocols can be implemented over the normal routing protocols such as AODV, DSR, and TORA.

Issues associated with trust based security mechanisms

- Though the trust mechanism is considered to be computationally inexpensive yet it is not as secure as its cryptographic counterparts.
- A lot of data storage and processing is required
- To calculate trust there is no single standard mechanism.
- The information that is provided in the form of second hand trust may not come from a reliable source.
- It takes time for the trust of a node to reach to a certain requisite threshold level so that the node can be regarded as trusted node.

3. THE PROBLEM

The trust rises very slowly and reaches to 1 asymptotically as shown in the Figure1. Let the minimum trust level be 0.6 so that a node can be regarded as trusted. This requires nearly 3 units of time (see Figure 1).Thus there is problem during period [0, 3] units when the adequate trust is not available and the cryptographic mechanisms have not been deployed.

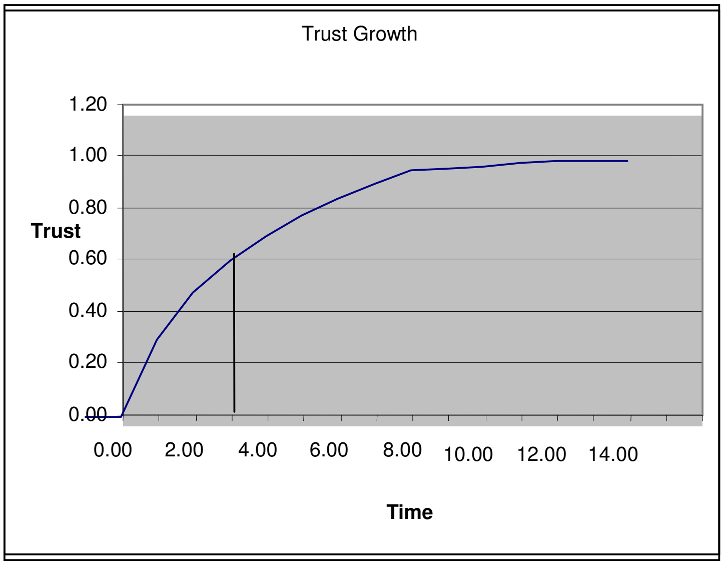


Figure 1. Growth of Trust

In this situation, there are followings options:

- Both strong cryptographic and trust methods are deployed with cryptography in initial stage and the trust at the later stage when it has reached the requisite level.
- Only trust is used and the traffic be allowed to go on and unchecked till the trust is established.

- Some intermediate solution be designed which can be used during the trust growth (up to requisite level) period.

The option 1 is very expensive and is not suitable as it requires both planned and unplanned management. The option 2 is a compromise with the security. The option 3 seems to be an amicable solution in such a situation. This paper is based upon a option 3 solution.

In this paper, we propose a light weight solution for security in MANETs based upon Random Electronic Code Book (RECB) and permutation functions. The method is efficient because it does not involve multiple rounds of sequential mechanism as in case of Feistel type structures [24] as used in Symmetric cryptography. Moreover, it involves the sharing of comparatively large amount of information which is much more than a single key making it difficult to grab. The next section provides full details about RECB and other aspects of implementation.

4. PROPOSED SECURITY SOLUTION

The heart of the proposed security mechanism is the random electronic code book (RECB). This code book is used for converting the plaintext to the cipher text. The RECB contains 16 bit unique random cipher code for each 16 bits of plaintext information. There is no mathematical or logical relationship between the intermediate cipher text and plaintext and the mapping between the two is one to one. The only way one can get the cipher text corresponding to a plaintext is through the matching process in RECB. Figure 2 shows the basic structure of the RECB. The codebook can be generated through a simple algorithm. It may however be pointed out that most of the computers generate the random numbers in the pseudo manner and the success of this mechanism is likely to increase with the truthfulness of the random number generation process. The literature contains many strategies to accomplish this[28, 29]. These strategies, though not perfect, yet give quite good result.

Since for each word of 16 bit in the RECB there are 216 possibilities, hence the total number of possible code books are 2^{16} X 2^{16}=2^{32} > 4X10^{18}, which is quite a huge number keeping in view the brute force search.

Plain text	Random Cipher code
0000h	8fdah
0001h	8423h
0002h	4231h
------	------
------	-------
------	--------
------	------
------	-------
Ffffh	89f3h
H indicates hexadecimal notation	

Figure. 2 Structure of Random Electronic Code book

The proposed security solution can be applied above almost all basic routing protocols used in MANETs, may it be reactive or proactive. All the nodes which are the initial members of the network are given the RECB and the permutation codes. To create a route between a source node S and the destination node D the source S asks its neighbour, does it posses the RECB. If yes, the node is trusted one and is eligible for being included in the route. The possession of the RECB is verified by the exchange of challenge/ response mechanism where by the source node asks its neighbour to respond to a challenge word through the random cipher code contained in RECB. The neighbour is included in the list of trusted nodes with the initial value of trust index. Now the data packet is transmitted and the neighbour is put in the promiscuous mode to check its behaviour for the packet forwarding. The malevolent or benevolent behaviour of the neighbour nodes is used for altering the trust index.

If the neighbour node doesn't posses the RECB then the source node asks to submit its identity and other credentials. If the source node is satisfied then it gives the new node the RECB and the permutation codes which establish the new node in the network. The process is somewhat similar to [26] wherein the public key is distributed on the basis of personal acquaintance. This eliminates the requirement of central agency, a major hurdle in the implementation of security feature in ad hoc networks.

The RECB serves following purposes

- It establishes the new node in the network with initial level of trust.
- There is no need for central authority during the operational phase of the network.
- Scalability of the network is not hindered.
- It can be used to encode the data packet contents using the random cipher code

4.1. Packet Format

A data packet is of the size 1024 bits which contain header, payload and the padding as shown in Figure 3.

Header	Payload	Padding

Figure 3. Packet Format

Pkt type=data packet
Pkt size= 1024 bits
Header size= 128 bits
Payload=actual data size= max permissible=1024-128=896 bits. If payload is lesser than 996 bytes pad with 10000………...
This packet is now divided into 8 blocks each of 128 bits as shown in Figure 4.

Block 1 (128 bits)	Block 2 (128 bits)	Block 3 (128 bits)	Block 4 (128 bits)	Block 5 (128 bits)	Block 6 (128 bits)	Block 7 (128 bits)	Block 8 (128 bits)

Figure 4. Division of packet into blocks

Each block is divided into 8 words of size 16 bits as shown in Figure 5. All the words of the block are given a random cipher code using RECB except the first block that contains the header information.

Word1	Word2	Word3	Word 4	Word5	Word6	Word7	Word8
16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits	16 bits

Figure 5. Division of each block into 8 words of 16 bits

The random cipher code words are now subjected to a permutation function. This permutation function scrambles the words within the block. For example, suppose we have a block having the permutation function given as (6,1,2,7,8,4,3,5) then the corresponding permuted block will be (2,3,7,6,8,1,4,5). This process is shown in Figure 6. It implies that the first word is to be placed at the sixth place, second at the first place and so on. For each block 8! = 40320 permutation functions are possible.

Original word order	1	2	3	4	5	6	7	8
Permutation function f_i	2	3	7	6	8	1	4	5
Permuted word or block order	2	3	7	6	8	1	4	5

Figure 6. Permutation function used for inter-block or intra-block permutation

Each block except the header block uses a separate permutation function fi i.e. there are total permutation functions namely f_1, f_2, f_3, f_4, f_5, f_6 and f_7 for intra-block permutation of words. After this intra-block permutation of words, the blocks are permutated using a 7 argument permutation function F in the similar manner as described above. The permutation function F is applied on all the blocks except the header block. The permutation process uses eight permutation operations in all, seven for intra-block permutation and one for inter-block permutation

4.2. Encryption algorithm

```
1.      Receive Plaintext message
2.      Make 1024 bit packet by adding header and padding.
3.      Divide the packet into 8 blocks of 128 bit each.
4.      Divide each block into 8 plaintext words of 16 bit each.
5.      For each block i (i=2; i<=8; i++)  /* header block not permutated */
{
For each word j
{
cipher_text (i, j) = recb(plaintext(i, j);
}
        Apply intra-block permutation on block i using function $f_i$
}
6.      Apply inter-block permutation function F on each block except the header block
7.      Transmit secured message
```

4.3. Decryption Process

When the packet is received at the destination, the packet is subjected to inter-block anti-permutation operation using the function anti_F. The application of anti_F reorders all the blocks in their original order. Each block except the first block which contains the header information is now subjected to a anti-permutation function anti_fi to bring each word in the original order. Figure 7 shows the application of anti-permutation function anti_fi.

Permutation function f_i	2	3	7	6	8	1	4	5
Anti Permutation function anti_ f_i	6	1	2	7	8	4	3	5
Original block or word order	1	2	3	4	5	6	7	8

Figure 7. Anti-permutation function for intra block anti permutation

4.4. Decryption Algorithm

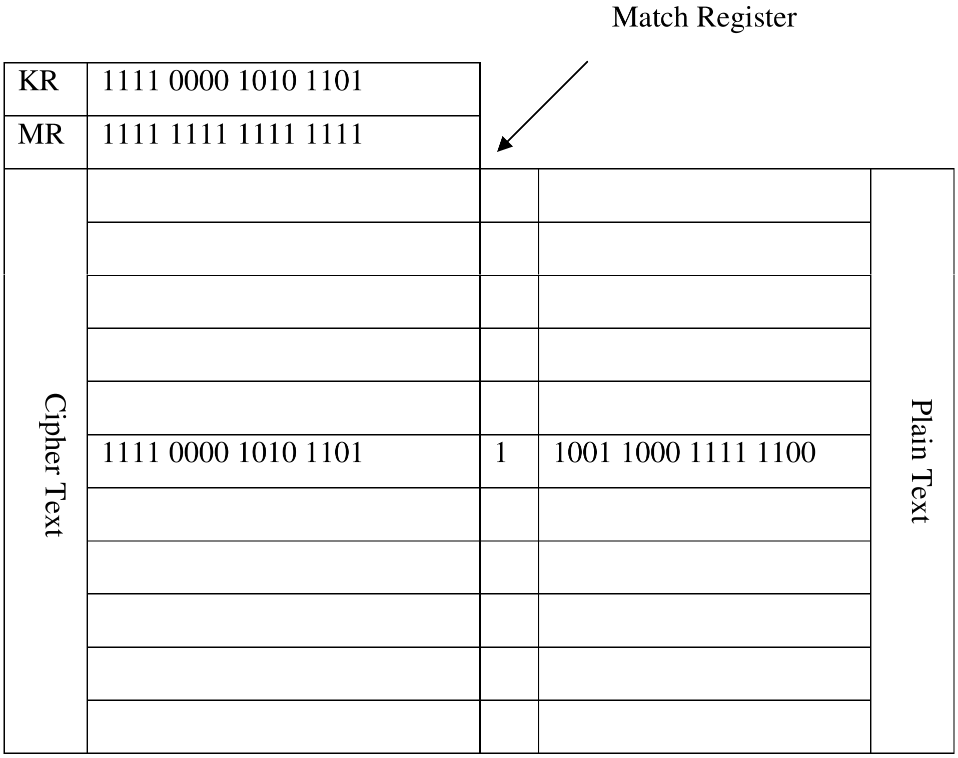
```
1.        Receive Secured Message Pkt
2.        Divide the pkt. into 8 blocks of 128 bits each.
3.        Apply inter-block anti permutation function Anti_F
4.        Divide each block into 8 sub-blocks of 16 bit each.
5.        for each block i
{
Apply intra-block permutation on block i using anti permutation function ant_$f_i$

for each 16 bit word j in block i
          {
plain_text (i,j)=inverted_recb_search (cipher_text (i, j))
}
}
6.         Use plaintext message
```

For the conversion of cipher_text into plain text, there are two design possibilities:

1. Each node being trusted after requisite scrutiny is provided with the inverted list which is inverse of RECB that maps the cipher code to plain text.
2. The plaintext code can also be obtained by using a content addressable memory (CAM), containing a mapping between the cipher code and the plain text. The intermediate cipher code word can be put in the key register of the CAM and corresponding plain text can be found. The arrangement is shown in Figure 8.

We propose the use of second mechanism as it uses parallel matching which is quite quicker then the first one.

The RECB and inverse RECB are software implementable using array in any language and can be created in any devices and be circulated. The CAM is hardware implementable and can be created if dedicated devices are being manufactured.



KR	1111 0000 1010 1101
MR	1111 1111 1111 1111

1111 0000 1010 1101	1	1001 1000 1111 1100

Figure 8. Parallel matching of intermediate cipher code with Plain text using CAM

5. CONCLUSIONS

An Ad hoc network is formed by a number of wireless nodes with limited energy, transmission power and the computational power and their capability to operate without any fixed infrastructure. Every node in the network helps others by forwarding packets for them. If every node performs its duty well there is no problem. However in the lack of fixed infrastructure and stringent rule for membership it is quite possible that malicious nodes also get a chance to participate in the network. These nodes can carry out a variety of attacks on the network and hamper its operation. To counter these nodes cryptography based schemes can be applied which are quite secure but these schemes put a number of prerequisites on the network both during the installation phase and operational phase. Also there is a deviation from the ad hoc concept in which the network is established in a spontaneous and impromptu manner. To overcome this drawback of the cryptographic technique trust based methods have been proposed wherein the behaviour of each node is observed by the other nodes in the network and the collected information is used to develop a trust index about the node. However, it takes time for the trust to grow to a requisite level, so there has to be a mechanism to secure the network during this period. The dynamic sharing of the RECB, inverted RECB and permutation function ensures that the initial critical period is passed without the intervention of non trusted nodes thus ensuring the safety of the network.

ACKNOWLEDGEMENTS

The authors would like to thank all nears and dears who have been source of inspiration to them.

REFERENCES

1. Wireless LAN media access control (MAC) and physical layer(PHY) specifications, IEEE Standard 802.11, First edition, 1999
2. Rafael Timoteo de Sousa Jr., Robson de Oliveira Albuquerque, Maíra Hanashiro, Yamar Aires da Silva and Paulo Roberto de, Lira Gondim, “Towards Establishing Trust in MANET: an Integrated Approach for Auto-configuration, Authentication and certification” International Journal of Forensic Computer Science, IJoFCS(2006) I, 33-40
3. Brian B. Luu, Barry J. O’Brien, David G. Baran, and Rommie L. Hardy” A Soldier-Robot Ad Hoc Network” Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PerComW'07)
4. C.E. Perkins and E.M. Royer. Ad hoc on demand Distance Vector routing, mobile computing systems and applications, 1999. Proceedings. WMCSA ’99. Second IEEE Workshop on, 1999, p90 - p100.
5. Murthy, S. and J.J. Garcia-Luna-Aceves, An Efficient Routing Protocol for Wireless Networks, ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.
6. L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, Nov. 1999.
7. S. Marti and T. Giuli and K. Lai and M. Baker, “Mitigating Routing Misbehavior in Mobile ad hoc networks,” in The Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA, USA, Aug. 2000.
8. F. Wang, B. Vetter, and S. Wu. Secure routing protocols: Theory and practice. Technical report, North Carolina State University, May 1997.
9. C. Perkins, E. Belding-Royer, and S. Das. RFC3561: ad hoc on-demand distance vector (AODV) routing. Internet RFCs, 2003.
10. D.B. Johnson, D.A. Maltz, J. Broch, et al. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5:139–172, 2001.
11. Z.J. Haas. A New Routing Protocol for the Reconfigurable Wireless Networks. In Proceedings of the IEEE International Conference on Universal Personal Communications (ICUPC, pages 562–566, 1997.
12. C.E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Computer Communication Review, 24(4):234–244, 1994.
13. Y.C. Hu, D.B. Johnson and A. Perrig, “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks,” IEEE, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’02), 0-7695-1647-5, 2002.
14. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM’02, 2002.
15. P. Papadimitratos and Z.J. Haas. “Secure routing for mobile ad hoc networks,” SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.
16. B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad hoc networks,” in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.
17. ftp://MANET.itd.nrl.navy.mil/pub/MANET/2001-10.mail, October 8, 2001.M. Zapata, N. Asokan, “Securing ad hoc routing protocols”, WiSe’02, ACM 1-5813-585-8, September 28, 2002, pp.1-10.

18. S. Marti, T.J. Giuli, K. Lai, and M. Baker. “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000, pp.255-265.
19. S. Buchegger and J. Le Boudec, “Performance analysis of the CONFIDANT protocol: (Cooperation of nodes - fairness in dynamic adhoc networks),” in Proc. IEEE / ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc'02), Lausanne, Switzerland, June 2002, pp.226-336.
20. P. Michiardi and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” Communication and Multimedia Security Conference (CMS'02), September 2002.
21. Q. He, D. Wu and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", in Proc. IEEE WCNC2004, Mar. ’04.
22. S. Bansal and M. Baker, “Observation-based cooperation enforcement in ad hoc networks,” Research Report cs.NI/0307012, Stanford University, 2003. (ocean 22)
23. A. A. Pirzada, C. McDonald and A. Datta, “ Performance Comparison of Trust Based Reactive Routing Protocols” IEEE transaction on mobile computing, Vol. 5, No. 6, June 2006, pp 695-710.
24. “Cryptography and Network Security: Principles and Practices”, William Stallings, Pearson Education, First Indian Reprint, 2003.
25. “Introduction to Automata Theory, Languages and Computation” , J. E. Hopcroft, Rajeev Motwani, J. D. Ullman, Pearson Education Second impression 2009.
26. S. Capkun, L. Buttyan, and J. P. Hubaux, “ Self Organised Public Key Management for Mobil Ad hoc Networks” IEEE transaction on Mobile Computing, Vol. 2, No. 1, Jan 2003, pp 52-64.
27. “Ad hoc Wireless Networks: Architectures and Protocols”, C. S. R. Murthy and B. S. Manoj Pearson Education Fourth impression 2009.
28. www.random.Org
29. http:\\www.robertnz.net/true_rng.html

Authors

Shailender Gupta is B.Tech. (Electronics) and M.Tech.(Computer Engg.) and pursing his Ph.D. in the area of ad hoc mobile network security. His academic interests include network security, automata theory and fuzzy logic.

Chander Kumar is M.Tech.(Computer Engg.) and Ph.D.(Comp. Science). His academic interest include network security, software reliability and artificial intelligence

.