Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 10 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Time Stamp Based Cross Layer MANET Security Protocol

By Gaurav Kulkarni & Brajesh Patel
Shri Ram Institute of Technology, India

Abstract - Mobile Adhoc Network (MANET) is a wireless network where nodes communicate through other nodes without the aid of a base station. Security is a major challenge in MANET as the packets are prone vulnerability and eavesdropping in wireless environment. Generally MAC layer provides the security in such wireless network through encryption and authentication and the protocol is called WEP. Many authentication and encryption techniques are proposed to increase the security of the MANET. But stronger Security leads to more energy loss as mobiles have less energy and limited processing capability. In this work a Cross layer timestamp based network security technique is developed. The technique reduces the encryption packet overflow which is due to PKE or public key exchange, and derives the public key directly from the neighbor's table which is transmitted using routing information exchange. The simulation is performed with omnet++ simulator. Performance results demonstrate that the energy overhead due to encryption or performance compromise are very low in the proposed system. Further as the protocol is embedded in the network layer it is easily adoptable to any existing architecture without modifying the MAC or Physical layer standard or protocol.

Keywords : AODV, cryptography, MANET, time stamp, wireless security.

GJCST-E Classification : C.2.2

TIME STAMP BASED CROSS LAYER MANET SECURITY PROTOCOL

Strictly as per the compliance and regulations of:

Time Stamp Based Cross Layer MANET Security Protocol

Gaurav Kulkarni [α] & Brajesh Patel [σ]

Abstract - Mobile Adhoc Network (MANET) is a wireless network where nodes communicate through other nodes without the aid of a base station. Security is a major challenge in MANET as the packets are prone vulnerability and eavesdropping in wireless environment. Generally MAC layer provides the security in such wireless network through encryption and authentication and the protocol is called WEP. Many authentication and encryption techniques are proposed to increase the security of the MANET. But stronger Security leads to more energy loss as mobiles have less energy and limited processing capability. In this work a Cross layer timestamp based network security technique is developed. The technique reduces the encryption packet overflow which is due to PKE or public key exchange, and derives the public key directly from the neighbor's table which is transmitted using routing information exchange. The simulation is performed with omnet++ simulator. Performance results demonstrate that the energy overhead due to encryption or performance compromise are very low in the proposed system. Further as the protocol is embedded in the network layer it is easily adoptable to any existing architecture without modifying the MAC or Physical layer standard or protocol.

Keywords : AODV, cryptography, MANET, time stamp, wireless security.

I. Introduction

a) Mobile Adhoc Network

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably. MANETs are usually set up in situations of emergency for temporary operations. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication. MANET has greater security risks than conventional infrastructure networks, we adopt Adhoc on demand Distance Vector (AODV) [20] protocol for routing in MANET and embed the proposed security credentials over the protocol [24].

II. Problem Formation

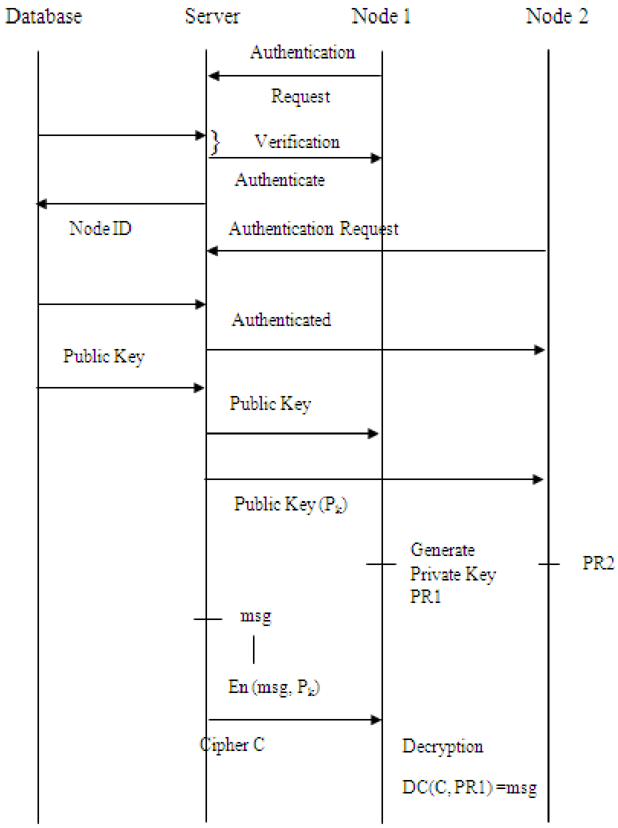

Figure 1 : Sequence diagram of conventional encryption technique

The most adoptable form of cryptography is as depicted in figure 1. It can be understood from the figure that the task of distribution of the key is the role of the server. Once server authenticates peers, then only it can distribute the key. Hence at the beginning security essentials must be exchanged. After the key is distributed amongst all the authenticated nodes, authenticated nodes use the public key to encrypt any message they want to transfer to the other peers and the encrypted message or the cipher is decrypted at the other end using the private key of the node. Further public keys can be changed in a subset called a group [16] and the common key is called a group key.

Author α : ME (SS) – IV Semester Department of ME/ M.Tech, Shri Ram Institute of Technology, Jabalpur (MP), India.
E-mail : kulkarnigaurav@yahoo.com
Author σ : Department of ME/M.Tech, Shri Ram Institute of Technology, Jabalpur (MP), India.
E-mail : brajesh.patel@rediffmail.com

The basic problem with the existing protocol is extensive amount of data exchange for authentication and requirement of excessive processing power for strong encryption techniques. Both of these leads to bandwidth consumption and subsequently delay in initial packet transmission, and excessive energy [11] loss due to higher processing cycles for encryption. More security invariably increases the latency, where as less strong encryption mechanism results in more eavesdropping. In order to have a balance between the security and performance, generally either the quality of transmission is sacrificed or strength of the key is satisfied or the encryption mechanism is compromised. Moreover in any technique, it is suggested that the key used for encryption be refreshed periodically (at least once in every 30 minutes).

III. Proposed Technique

a) General Architecture of the System

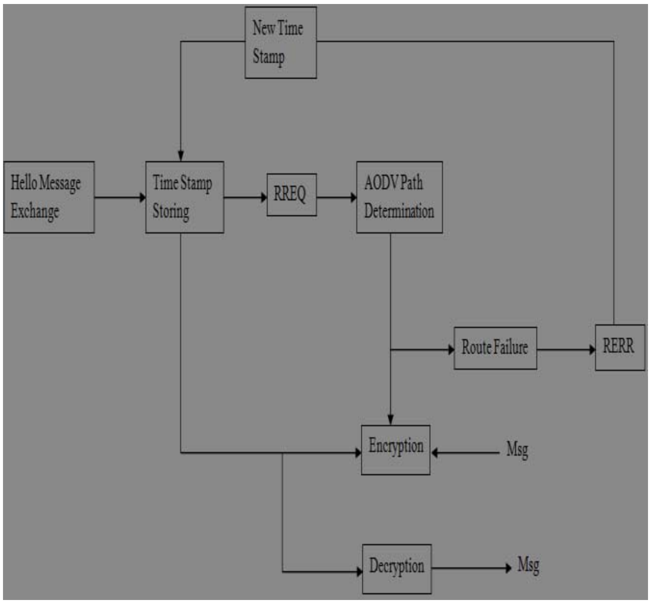

Figure 2 : Generalized Diagram of Proposed Technique

Figure 2 describes the architecture of the system. The MANET architecture is considered to be an autonomous topology without any base station or cluster head [18] [19]. Nodes set a future time when it is going to generate the hello message and stores that time value. This is propagated to all the neighboring nodes, they store the same value. Once the route is established every node in the route encrypts the message with the key generated from the time stamp of the next hop and so on. If there is a route error due to factors like the mobility or power issues a Route Error (RERR) message is generated. Once this is propagated to the source node, source node generates the RREQ message with the new time stamp and new sequence number. All the nodes receiving this RREQ further update the neighbors table along with the new time stamp value. Hence automatically the key is changed without any overhead of key refreshing [27]. Further after the hello interval is expired (which is typically 3 seconds) the hello messages are again exchanged between the nodes and the keys are further updated. The process is elaborated in more detail in the next subsection.

b) Functioning of Independent Sequences

1. The node exchange hello message at the start of the network or session to build the routing table or neighbor table.
2. We propose a new hello packet structure where a node appends transmission timestamp in the hello packet and broadcast the hello packet.
3. Each node notes down its transmission timestamp for the hello packet.
4. Once the hello packet is received by the node, it makes a routing table entry for the sender node. We device a time stamp based hash generation technique. Once all the nodes receiving the hello packets from the sender node, makes a table entry of the sender nodes id and the transmission time stamp. This time stamp acts like the public key between the sender and the receiving nodes. When the sender intern receives the hello packet from all these nodes which had received hello packet transmitted by the sender, sender also makes a table entry of these nodes and corresponding time stamps. Therefore in a session there is a single pair of base function for generating the key between any two nodes.
5. Now we assume that a node joins right at the middle of hello message exchange and acquires the time stamp values of the neighboring nodes. If this node is not an authenticated node, it will not be preloaded with the hash generation method and needs time for guessing the hash in the course of any data exchange between valid nodes. Hello interval in Adhoc network is generally kept at three seconds. Hence in every three seconds the base pair between any two nodes gets changed thus making it impossible for the intruder to guess the hash.
6. Another type of threat that might occur in the network is that an unauthenticated person gets access of a valid device of the network and hacks the data even being unauthenticated. In a centralized system this problem is solved through authentication protocol. In authentication protocol, the user enters his authentication information like username and password which upon matching with a central storage, the system authenticates the user and the device can subsequently take part in the communication. In a decentralized method such authentication scheme cannot be adopted. Hence we propose a unique technique of client side authentication. Whenever a wireless packet is

received by the device for the first time (Either a hello packet or a route request packet or a data packet, the device asks for authentication credentials. Once the credential is true, the device is self authenticated and is made part of the network. Authentication credentials are stored in the device itself when the user accesses the network for the first time by issuing "join network" command.

7. Three attempts are given for the user to successfully enter the authentication credentials. After three attempts, the device is unauthenticated for a period of 15 minutes and the same process is repeated.
8. In the most common possible attack of this type, when the unauthenticated user tries to access the network for the first time, his authentication credentials are asked. This method cannot check is the user entering new credential is valid user or not. Hence the user whenever wants to join the network needs to get a key from the system administrator. This key may be provided as a scratch card or a "on the fly" number. This number is generated from the MAC address of the device and current time frame. A time frame of four hours is selected as the time interval frame for which this number will be valid. Thus the user can authenticate only this device and only within four hours of issuing of the number.
9. Hence there is no significant overhead in key exchange and authentication data exchange. The strength of the algorithm can be moderate as against the desired very strong encryption technique for other methods because key refresh rate is very high over here.

c) Time Stamp Based Mechanism

[7] Defines a time stamp based mechanism whereby the digital document is signed with a time stamp. The time stamp is either a local time stamp or a time stamp generated from a time stamp server. But as the authentication phase is not considered to be QOS [22] supportive in MANET environment, rather than signing the document with a time stamp, we propose a technique to generate a key from unique time stamp values. [2] Describes a mechanism for a security mechanism where a signature or hash is generated from two numbers on the basis of RSA algorithm.

1. Generate two large primes p and q and compute $n = pq$.
2. Choose a prime number e and an integer d such that $e.d \bmod (p - 1)(q - 1) = 1$.

Where e is the system public key, d is the corresponding private key, which should be provided to server in safe way.

3. Find an integer g, which is a primitive element in both GF (p) and GF (q) and the public information in the system.

In the proposed system the time stamp values is first converted into a long time format which is a unique long number. This number is converted into string and inversed. The inverted string is converted back into the number and a prime number is generated which is just bellow this number and just above this number. This two primes P and Q are unique. Now two keys d and e must be obtained such that it satisfies the condition as 2.

In a standard protocol e must be submitted to the server securely (a technique of key distribution is elaborated in [10]) because P and Q may be any random number. In case the key is lost due to bit errors in the channel they can be recovered using key recovery technique like [13]. Even though such techniques do not require modifying existing Secured Socket Layer (SSL) protocols, key recovery is time consuming and adds extra latency to packet transmission.

[15] suggest a way to enhance the security by generating new signature by aggregating the old signature values which requires old values to be stored and the mobility in the network makes it difficult for all the nodes to have same set of old signature in order to generate a new unique signature. Hence the fresh time stamp is considered and no aggregation is selected. But in the proposed system as P, Q are unique based on a specific time stamp, e is not needed to be transferred to any other node.

d) Comparison between Proposed Technique and Existing Technique

In order to reduce the authentication overhead conventional security mechanism like Secure Ad hoc On-Demand Distance Vector (SAODV) compromises on the authentication issues and concentrates only on the encryption technique. Therefore there is always the possibility of unauthenticated nodes joining the network at the time of key exchange and acquires the public key which then enables these nodes to hack the packet for the validity of a route life time. But the proposed system removes this option. Only the Nodes valid in the route and along the forward path get the key along with the Route acknowledgement. Another benefit of the proposed system is that no key is exchanged in actual transmission, rather they are locally generated from the time stamp value transmitted by the nodes. Therefore extra security for the keys is not required. Further no extra bandwidth is consumed for key transmission. The key generation base that is the time stamp values are embedded in the existing packet headers, reducing the bandwidth overhead due to cryptographic extension.

IV. Simulation and Results

a) Simulation Mechanism

The proposed system is simulated with omnet3.3 in windows environment. The parameters used in the simulation are listed in table 1. Randomly N nodes are placed over an area of 500x500 meters. MAC layer protocol is 802.11b with 11.2 mbps data rate. First for authentication purpose, unique authentication credentials must be generated for every node. Therefore a pool of 100 MAC addresses of 48 bit is configured in the network with MAC ID like 80:50:1b:48:b3:c1: 80:50:1b:48:b3:c100. For time stamp generation, current system time is converted into long unique integer and is used with the simulation time. Once the network starts, the network layer of each node schedules a HELLO event for sending the hello packets to its neighbors. The scheduled time is noted down by this node and is also embedded in the HELLO packets. The device ID and a unique number allocated by the network administrator to these nodes are also embedded in the packet. When a node receives the HELLO packet from its neighbors, it generates the required authentication credential from the device id, time stamp and the unique number and verifies if that is a valid authentication credential or not. In order to simulate this we use the last numeric value from the MAC address of the node and multiply this with the last numeric value of the unique number which is of form [A10b21]. The generated numbers must lie between 1 to 1000. Further it is divided by validation period of the key which is maximum four hours (i.e. 240 minutes). Therefore all the authenticated nodes must fall in the range of 0 to 5. Further to show the presence of unauthenticated nodes and the detection and rejection of such nodes in the course of simulation, we place N/3 nodes along with N valid nodes with MAC address not in the range of the valid MAC addresses for the network. Even if they generate their hello packet, neighbors reject the hello packet due to un-authentication and thus these nodes are never selected in the neighbor table. Hence they do not get any Route Reply Acknowledgment (RREP-ACK) with the actual time-stamp of the source node, as the RREP-ACK packets are uncased.

The primary simulation objective is to show that even by embedding security essential in the wireless network and extending the existing routing protocol with the proposed security enhancement, network performance remains acceptable and that there is no unnecessary overhead for packet transmission or no "over-energy" consumption issues are observed due to the security enhancements. Therefore simulation results are obtained for both Conventional AODV and proposed Technique.

b) Simulation Parameters over omnet.

Parameter	Value
Nodes	5-35
Sessions	5-20
Pause time(seconds)	50-300
Packet Rate(per second)	20packets/second
Packet length	4096 bits
MAC protocol	802.11b
Bandwidth	11.2 Mbps
BER	1x10 -6
Initial energy	1000 m Joules
Area	500x500 square meter
Routing Algorithm	AODV
Transmission power	5mWatt/Packet
Simulator	OMNET++
Control Message Length	1 byte Identity, 8 bytes time stamp
Hashing Technique	RSA Based

Table 1 : Specifications of constraints included in simulation

c) Algorithm to demonstrate energy transmission

Let N be number of nodes, S be the source and D be the destination. Et be the transmission energy for 1 m distance, Er be the received energy for 1m distance. Let P packets are to be transmitted.

```
K=0;
For i=1:1: N
Transmit HELLO packet along with time stamp.
K++;
End
handleHello:
for i=1:1:K
for j=1:1:N
Store Tj at i
Prepare neighbor table
end
end
// now source transmits RREQ packets
For i=1:1:N
handleRREQ:
for(j=1:1:length(Neighbour_Table))
Forward_RREQ to j
If j is destination,
Send RREP
If(j==source && j has received RREP)
Generate ACK; //where ACK is route acknowledgement
end
//Data transmission phase
// let message be MSG
for j=1:1: number of nodes in the path
if(i==1)
C=EN(MSG,Ti+1)
Send C
Else
If(i!=destination)
```

```
D=DC(C,Ti)
C=EN(D,Ti+1)
Send C
end
end
end
end
```

Where EN and DC are encryption and decryption function.

V. Results

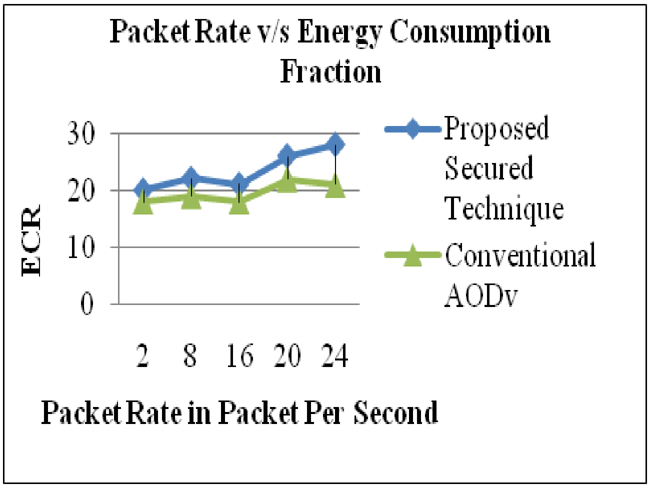

Figure 3 : Packet Rate v/s Energy Consumption Fraction

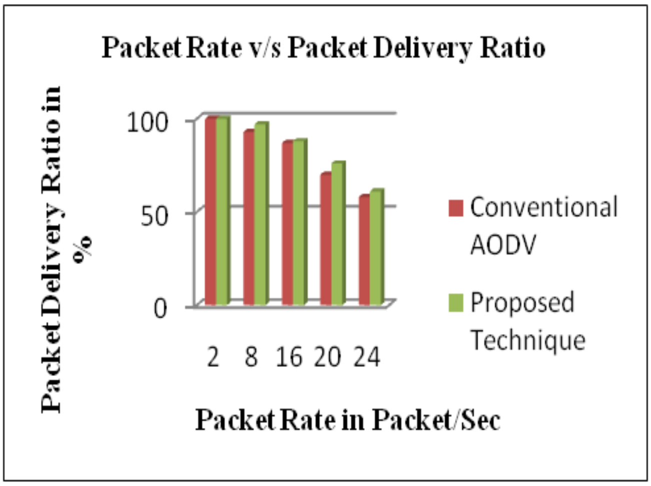

Figure 4 : Packet Rate v/s Packet Delivery Ratio

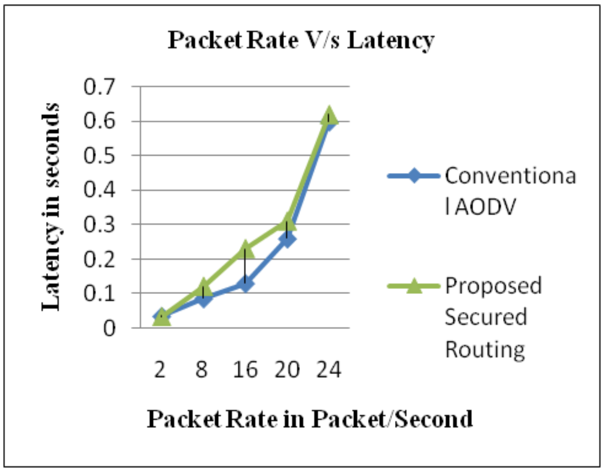

Figure 5 : Packet Rate v/s Average Latency

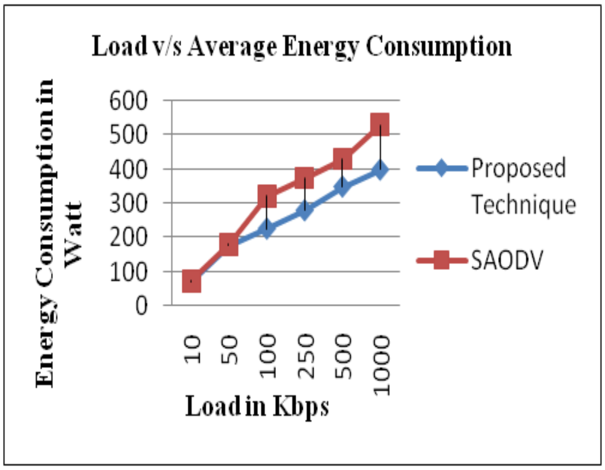

Figure 6 : Average Energy Consumption in SAODV and Proposed Technique

Average energy consumption is derived as (total energy of the nodes at the beginning of simulation –total energy of the nodes at the end of simulation)/total number of authenticated node.

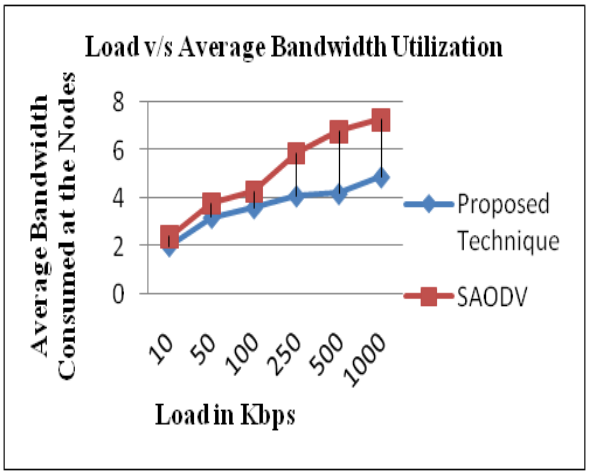

Figure 7 : Load v/s Average Bandwidth Utilization in SAODV and Proposed Technique

VI. Conclusion

The basic objective of the proposed technique is to show that even by introducing security features, quality of service is not compromised in the proposed method. Result 1, 2 and 3 shows that packet delivery ratio, latency and energy consumption fraction which is defined as the energy spend by control messages over energy spent by data messages are at par with the conventional technique and latency result is better in the presence of intruding nodes. This proves that the proposed technique can be adopted in AODV without any compromise on the QOS issues. The comparison between the most adopted SAODV and the proposed system is most encouraging and it clearly shows that because there are no periodic key exchange in the proposed system, the bandwidth improvement is significant and also the energy consumed at the nodes are also less due to processing of lesser packets in comparison to SAODV. Further the latency improvement also suggests that because there are no overhead in exchanging extra security credential, network layer delay is kept minimum. Further the technique can be improved by incorporating QOS metric which can obtain a path which meets the QOS requirement and then applying the encryption mechanism over the same protocol.

References Références Referencias

1. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks”, Wireless/Mobile Network Security, Springer 2006.
2. Keerti Srivastava, Amit K Awasthi and R.C.Mittal, “An Improved Timestamp-Based Password Remote User Authentication Scheme”, Preprint submitted to Elsevier December 22, 2009.
3. Ajay Jangra, Nitin Goel, Priyanka & Komal Bhatia, “Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture”, International Journal of Electronics Engineering, pp. 189-196, 2010.
4. Guangyu Pei, Phillip A. Spagnolo and Fred L. Templin, “Enabling OSPFv3 MANET Extensions over IPv4 Encryptors”, IEEE 2008.
5. Levente Butty´ana, L´aszl´o D´ora, Fabio Martinelli, Marinella Petrocchi, “Fast Certificate-based Authentication Scheme in Multi-operator maintained Wireless Mesh Networks”, Preprint submitted to Elsevier Computer Communications January 27, 2010.
6. Tao Ye, Darryl Veitch, Jean Bolot,” Improving Wireless Security Through Network Diversity”, Computer Communication Review, vol. 39, pp. 34-44, 2009.
7. Cryptomathic Time Stamping Authority Technical White Paper.
8. Greg Rose, “Combining Message Authentication and Encryption”, Qualcomm Australia, 2003.
9. Kshitiz Saxena, “The Analyses of Wireless Encryption Protocol- Proposed Enhancement to Handshake Mechanism in WPA”, Kshitiz Saxena / International Journal of Engineering Science and Technology, pp. 3657-3661, Vol. 2(8), 2010.
10. R. Murugan and A. Shanmugam, “Key Distribution System for MANET with Minimum Prior Trust Relationship”, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.
11. Jin-Man Kim, Jong-Wook Jang, "AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET," aict-iciw, pp.77, Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06), 2006.
12. SHU JIANG, “Efficient Network Camouflaging In Wireless Networks”, A dissertation Submitted to the Office of Graduate Studies of Texas A&M University, December 2005.
13. Rui-dan Su, Xiang-quan Che, Shao-feng Fu, Long-hai Li, Li-hua Zhou, "Protocol-Based Hidden Key Recovery: IBE Approach.
14. IPSec Case,” nswctc, vol. 2, pp. 719-723, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.
15. Li Zhao, “Enhance Communication Security In Wireless Ad Hoc Networks Through Multipath Routing”, A dissertation submitted for the degree of DOCTOR OF PHILOSOPHY, WASHINGTON STATE UNIVERSITY, School of Electrical Engineering and Computer Science, AUGUST 2007.
16. Duc-Phong Le, Alexis Bonnecaze, Alban Gabillon, “Sign timing Scheme based on Aggregate Signatures”, in ISI, pp. 145-149, IEEEE 2008.
17. Mohamed Salah Bouassida, Mohamed Bouali, “On the Performance of Group Key Management Protocols in MANETs”, Joint Conference on Security in Network Architectures and Information Systems (SAR-SSI‘07), Annecy (2007).
18. Harald H.-J. Bongartz, Tobias Ginzler, Thomas Bachran, Pere Tuset, “SEAMAN: A Security-Enabled Anonymous MANET Protocol”, RTO-MP-IST-083, UNCLASSIFIED/UNLIMITED.
19. Qian Fang, Ying Liu and Xiaoqun Zhao, “A Chaos–Based Secure Cluster Protocol for Wireless Sensor Networks”, pp. 522-533, Vol. 44, No. 4, Kybernetika, 2008.
20. R.PushpaLakshmi, Dr.A.Vincent Antony Kumar, “Cluster Based Composite Key Management in Mobile Ad Hoc Networks”, International Journal of Computer Applications (0975 – 8887) Volume 4 – No.7, July 2010.
21. C. Perkins and E. Royer,” Ad hoc on-demand distance vector routing”, IEEE WMCSA’99 (1999).

22. Sunam Ryu, Kevin Butler, Patrick Traynor, Patrick McDaniel, "Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems," ainaw, vol. 1, pp.519-524, 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007.
23. Anni Matinlauri, "Fairness and Transmission Opportunity Limit in IEEE 802.11e Enhanced Distributed Channel Access", Master's Thesis, HELSINKI UNIVERSITY OF TECHNOLOGY Faculty of Electronics, Communications and Automation Networking Laboratory", Espoo, 2008.
24. Jungwook Song, Sunyoung Han, "Mobile Node Authentication Protocolfor Proxy Mobile", International Journal of Computer Science and Applications, pp. 10 – 19, Vol. 6, No. 3, , 2009.
25. Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam, "Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology, 2006.
26. Haodong Wang Æ Qun Li, "Achieving robust message authentication in sensor networks: a public-key based approach", Wireless Netw, DOI 10.1007/s11276-009-0184-z, Springer May 2009.
27. Dr. Anil Kapil, Mr. Sanjeev Rana, "Identity-Based Key Management in MANETs using Public Key Cryptography", International Journal of Security (IJS), pp 1-8, Vol. 3, Issue 1.
28. S. Balfe, K. Boklan, Z. Klagsburn, and K.G. Paterson, "Key Refreshing in Identity-based Cryptography and its Applications in MANETs", In Proceedings of the2007 IEEE Military Communications Conference(Milcom 2007), 2007.
29. "Wireless Network Security", white paper, proxim wireless networks.
30. Nishu Garg, R.P.Mahapatra, "MANET Security Issues", IJCSNS International Journal of Computer Science and Network Security, pp.241-246, VOL.9 No.8, August 2009.
31. Sanket Nesargi, Ravi Prakash," MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", pp 1-10.
32. Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), pp 1-13, January, 2002.
33. Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, pp. 106-107, Vol.6, No.3, 2001.
34. Manel Guerrero Zapata, "Securing and Enhancing Routing Protocols for Mobile Ad hoc Networks.