ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient Mechanism for Securing Mobile Ad Hoc Networks Using Public Key Cryptography (PKC)

Vuppu Sravani
M.Tech Student
Department of CSE,
Sri Venkateswara College of Engineering and Technology.

Sanapala Bhaskara Rao, M.Tech
Associate Professor
Department of CSE,
Sri Venkateswara College of Engineering and Technology.

Abstract:

Security of networks depends on reliable key management systems which generate and distribute symmetrical/asymmetrical encryption/decryption keys between communicating parties. Traditionally, in wired networks, a central server is responsible to generate and distribute the keys securely. But because of no central server or fixed infrastructure exists in mobile ad hoc networks, there are many difficulties to carryout key management in dynamic and self organized mobile ad hoc networks. The dynamic change in topology results in the change of trust relationship among the nodes. In this paper, we have proposed a key management scheme in grouped network structure in which group leader of a group is randomly shifted, our scheme of key management doesn't require any trusted third party. The group leader is responsible to generate and distribute ids and public-private key pair to nodes. This method reduces the quantity of keys to distribute among the nodes. Using Public key cryptography (PKC) any of the two members of group can share a session key securely to communicate.

INTRODUCTION

The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center, and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges effectively.

In this paper, we circumvent these obstacles and close this gap by proposing a novel key management paradigm. The new paradigm is a hybrid of traditional broadcast encryption and group key agreement. In such a system, each member maintains a single public/secret key pair. Upon seeing the public keys of the members, a remote sender can securely broadcast to any intended subgroup chosen in an ad hoc way. Following this model, we instantiate a scheme that is proven secure in the standard model. Even if all the non-intended members collude, they cannot extract any useful information from the transmitted messages. After the public group encryption key is extracted, both the computation overhead and the communication cost are independent of the group size. Furthermore, our scheme facilitates simple yet efficient member deletion/ addition and flexible rekeying strategies. Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority render our protocol a very promising solution to many applications.

A MANET is a special type of wireless network in which mobile hosts are connected by wireless interfaces forming a temporary network without any

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

fixed infrastructure. In MANET, nodes communicate each other by forming a multi-hop radio network. Mobile nodes operate as not only end terminal but also as an intermediate router. Data packets sent by a source node can reach to destination node via a number of hops. Thus multi-hop scenario occurs in communication and success of communication depends on nodes' cooperation.

Security of a network is an important factor that must be considered in constructing the network. A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non repudiation. These security requirements rely on the availability of secure key management system in network. Fundamental goal of a key management system in a network is to issue the keys to the nodes to encrypt/decrypt the messages, to manage these keys and to prevent the improper use of legally issued keys. Absence of key management system makes a network vulnerable to several attacks [6]. Therefore, key management system is the basic and important need of a network for secure communication. A key management system normally involves key generation, distribution, updation and revocation of keys in network. The feature of MANETs such as dynamic topology, lack of centralized authority, resource constrained and node mobility are the major challenge in establishment of key management. Some techniques such as intrusion detection mechanism consume lot of nodes' battery power but cannot account for flexible membership changes. However, an efficient and secure key management system can solve this problem with an affordable cost.

On the hand, mobile ad hoc networking is multi-hop relaying, i.e. messages are forwarded by several mobile nodes from source to destination, if destination node is not directly reachable. In other words, nodes in MANET operate as not only end terminal but also as an intermediate router. Thus, multi-hop scenario occurs; where an attacker can insert, intercept or modify the messages easily in absence of secure routing protocol. This means that unprotected MANET is vulnerable to many attacks [21] such as wormhole attack [22], black hole attack [23] including node impersonation, message injection, loss of confidentiality etc.

In this paper, we proposed a key management scheme for group based MANETs in which a group leader can generate, distribute, update and revoke keys in its group and a provable secure routing protocol. Proposed key management scheme neither depends on a central server nor is it fully distributed. Our key management system forms a decentralized system that combines both centralized key management as well as distributed key management so that it can combine merits of both methods. Proposed key management scheme is a hybrid key management scheme that uses both Symmetric Key Cryptography (SKC) for secure communication and Public Key Cryptography (PKC) to authenticate other nodes and to share a session key.

LITERATURE REVIEW

A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network:

Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

An efficient group key management scheme for Mobile ad hoc networks:

Group key management is one of the basic building blocks in collaborative and group-oriented applications in Mobile Ad Hoc Networks (MANETs). Group key establishment involves creating and distributing a common secret for all group members. However, key management for a large and dynamic group is a difficult problem because of scalability and security. Modification of membership requires the group key to be refreshed to ensure backward and forward secrecy. In this paper, we propose a Simple and Efficient Group Key (SEGK) management scheme for MANETs. Group members compute the group key in a distributed manner.

System Analysis

Existing System:

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multi-hop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multi-hop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottom layer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company via WMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smart phones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers.

Disadvantages Of Existing System:

A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation center, and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges effectively.

PROPOSED SYSTEM:

Our contribution includes three aspects. First, we formalize the problem of secure transmission to remote cooperative groups, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints.

Second, we propose a new key management paradigm allowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints discussed above. The new approach is a hybrid of group key agreement and public-key broadcast encryption. Third, we present a provably secure protocol in the new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying.

Advantages of Proposed System:

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- First, the sender is remote and can be dynamic.
- Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients.
- Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients.
- Furthermore, it is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient.

PROPOSED KEY MANAGEMENT SCHEME

In this section, we proposed key management system for group based MANETs. Proposed key management scheme includes key generation, distribution and revocation phase. We make following assumptions:

- An offline Trusted Third Party (TTP) is available outside the network which is responsible only to issue a certificate and public/private key pair for mobile nodes.
- Intergroup communication is done through group leaders.
- Group leaders are trusted. Grouping algorithm is not periodic. This reduces updates and hence computation and communication cost in system.

Key Generation and Distribution

All group leaders in network are assigned a unique id. Each group leader has a public/private key pair and a secure hash function (for e.g. SHA or MD5). We define three types of keys in the network: Group key, key for all the members in group used to encrypt/decrypt all the traffic communicated in the group. Second key, a symmetric key shared between group leader and a member node of same group and third key, shared by all group leaders in network.

Group leaders generate group key for their groups independently. Group key is updated each time when a node joins or leaves the group to maintain the forward and backward secrecy. Second key (k) is shared between group leader and a member node at the time when node joins group. k is the function of node_id and a secret randomly generated number by group leader.

$$f(node\_id, N) = k$$

Where f is a secure hash function selected by group leader, node_id is assigned to a node at the time of joining and N is a secret number known only to group leader.

Third key is shared by group leaders in network. Group leaders can agree on a key to communicate securely using Group Diffie-Hellman key agreement protocol [13]. Key is updated when group leader election algorithm is invoked in any group; new elected group leader can start Group Diffie-Hellman key agreement to update the key.

Node addition

Whenever, a new node joins a group. It sends a request to group leader. This request might be captured by a malicious node showing as group leader to new node. Similarly, a malicious node can also send a request to group leader to join the group. Therefore, it is necessary for both group leader as well as new node to authenticate each other. Upon successfully mutual authentication, a node can join the group and share a key with group leader in a secure manner. A new node and group leader can authenticate each other using challenge-response protocol. New node sends a challenge to group leader and group leader provide a valid response to prove its genuinity.

Group leader selects two large prime numbers ‘p’ and ‘q’ and calculates: N=p*q, then selects a random secret number ‘S’ and calculates:V=S2 mod N (1<S<N).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

'N' and 'V' are publically announced in the group. When group leader has to authenticate itself i.e. it received a challenge from a node, it finds X=R2 mod N, where 'R' is a random number selected by group leader such that 1<R<N.

Group leader sends {N, V, X} to new node. On receiving (N, V, X), new node sends a challenge 'c' to group leader. Group leader calculates Y=RSC mod N and send it to node. Node calculates XVC and match with Y2. If both values are same, group leader is successfully authenticated.

After successful authenticating to group leader, new node can sends its certificate to group leader issued by offline TTP. Group leader verifies nodes' certificate, and extracts the public key of node from certificate. Group leader generates a node_id and sends node_id and a key generated by function f shared by group leader and node, encrypted with public key of new node. Group leader then update group key and group members list and sends to the members of group. Communication between group leader and new node takes place as follows:

A group of mobile nodes with a group leader of MANET is shown in Figure.2, where a new node 'A' wants to join the group. Following are the notations used in communication:

G ⟶ Group, {L, M}
M ⟶ Set of group members $\{m_1, m_2, m_3 \ldots m_n\}$
L ⟶ Group leader
A ⟶ New node
ID_A ⟶ A's Identity given by group leader
K_{XY} ⟶ Session key shared between node X and Y
e_X/d_X ⟶ Public key/Private key of node X
DS_X ⟶ Digital Signature of node X
T_X ⟶ Timestamp added by node X
$CERT_X$ ⟶ Certificate of node X
S_{LX} ⟶ Symmetric key shared between group leader and node X.
X: Y {k(M)} ⟶ Node X sends a message M encrypted with key k to node Y

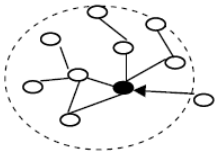

Figure 2. A Group in MANET

A : L {A, Join_req}
L : A ∪ M {N, V, X}
A : L ∪ M {c}
L : A ∪ M {Y}
A : L {$CERT_A$}
L : A {e_A (e_L, ID_A, S_{LA})}
A : L {S_{LA} (num}
L : A {S_{LA} (num, member_list, group key)}
L : M {group_key (new_group_key)}

Key Agreement Protocol

If a node A wishes to communicate securely with node B. Before starting communication, they must agree on a session key. A starts communication by sending message:

A: B {eB (IDA, IDB, TA, DSA)}

On receiving message from A, B decrypts the message and verifies the signature of A using public key of A. If node B does not have A's public key, it sends a message to group leader conveying to send A's public key. Here following two cases are possible:

- A is a genuine node and group leader has pubic key of A. In this case, group leader sends A's public key to B. B then verifies A's signature and share a session key KAB.
  B: A {eA (IDA, IDB, TA, TB, DSB)}
  A: B {eB (TA, TB, num1, KAB)}
  B: A {KAB (num1, num2)}
- In second case, A is malicious node and not a member of group. In that case, group leader would inform to all the member of group about node A.

Node Deletion

Nodes in a group communicate with group leader periodically showing its presence in group. If a node

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

doesn't communicate, group leader removes that node from member list and intimate other member. Group leader regenerates new group key and sends other nodes in group, encrypted by their public key. A node can be removed from member list when one of the following events occurs:

- A node can leave the group with prior notification.
- A node can leave the group without any prior notification or node is not forwarding the messages or performing as malicious node. Group leader exclude that node forcefully. In this case, group leader must inform to neighbor leader nodes.

On the other hand, whenever a group leader left the group with or without prior notification, a new group leader must be elected that can coordinate the group. New group leader reconstructs new group key and distributes in the group encrypted with the public key of members and share a new symmetric key with each member in group. New group leader distributes its public key and id to other group leader in network and starts Group Diffie-Hellman key agreement [13] to update key shared by group leaders.

PROVABLE SECURE ROUTING PROTOCOL

In this section we proposed a secure routing protocol in which source and intermediate nodes append their digital signature and hash code of received RREQ message to route request (RREQ) message and then rebroadcast RREQ message.

When neighbors of source receive RREQ, they verify the signature of source and make the decision accordingly. Destination sequence number [25] in the protocol is added to make the loop free routing and to check the freshness of route control packet. Source and destination node may or may not be in the same group. We discussed both cases i.e. intra group communication and inter group communication.

Intra Group Communication

Assume that S is the source node trying to discover a route to destination D. A and B are two intermediate node. All nodes are in the same group.

Notations:

1) $L_{RREQ} \rightarrow$ Life time (maximum number of hops) of RREQ.
2) $Seq \rightarrow$ Destination sequence number.
3) $DS_A \rightarrow$ Digital Signature of node A.
4) $h_A \rightarrow$ Hash code appended by A to RREQ.
5) $A \rightarrow *$ A broadcasts message.
6) $A \rightarrow B$ A sends message to B.
7) $H \rightarrow$ Hash function

Route Discovery:

1) $S \rightarrow *$ RREQ $(S, D, Seq, L_{REQ}, <S>, DSs, h_S)$
2) $A \rightarrow *$ RREQ $(S, D, Seq, L_{REQ}-1, <S, A>, DSs, DS_A, h_A)$
3) $B \rightarrow *$ RREQ $(S, D, Seq, L_{REQ}-2, <S, A, B>, DSs, DS_A, DS_B, h_B)$
4) $D \rightarrow B$ RREP $(S, D, Seq, <S, A, B, D>, DSs, DS_A, DS_B, DS_D, h_D)$
5) $B \rightarrow A$ RREP $(S, D, Seq, <S, A, B, D>, DSs, DS_A, DS_B, DS_D, h_D)$
6) $A \rightarrow S$ RREP $(S, D, Seq, <S, A, B, D>, DSs, DS_A, DS_B, DS_D, h_D)$

Description

Source S initiates route discovery process by generating route request (RREQ) message. On every broadcast of RREQ, life time of RREQ would be decreased by one. RREQ would be discarded if life time reached to zero. Source appends its Digital Signature (DSS) and hash code hS. = H(S, D, Seq, LRREQ).

When a neighbor of S, say A receives the RREQ message, it verifies the signature of S. and appends its identifier A to route list and its Digital Signature (DSA) to RREQ and replaces hS by hA= H(hS, A, LRREQ-1).

Similarly, next node B verifies signatures of node(s) of route list and then appends its identifier B and Digital Signature (DSB) to RREQ, and replaces hA by hB= H (hA, B, LRREQ-2).

Finally, when destination D receives the RREQ, it verifies all the signatures; it computes hash code hD to check integrity of RREQ:

hD = H(B, LRREQ-2 H(A, LRREQ-1 H(S, D, Seq, LRREQ)))

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This must be same as hB. If both values are same, D sends back route reply (RREP) message to B towards S. Otherwise discards RREQ. When S receives RREP, S verifies signature of all nodes S also computes hash code h to check message integrity:

h = H (B, LRREQ-2 H (A, LRREQ-1 H (S, D, Seq, LREQ)))

h must be same as hD. Otherwise RREP is discarded by S.

CONCLUSION

In this paper, we proposed a key management scheme and a secure routing protocol for mobile ad hoc networks. We described a secure key management system for group based a mobile ad hoc network that does not rely on a centralized authority for generating and distributing keys. Group leaders generate, maintain, and distribute the keys in their groups in a secure manner. Challenge- response protocol allows a new incoming node to authenticate to group leader, then joins group. Proposed routing protocol uses hash function to maintain the integrity of message. Therefore, any kind of modification in RREQ can be detected. Using Public Key Cryptography (PKC), nodes can negotiate the session key for secure communication that fulfills the requirement of confidentiality. Security analysis results show that protocol establishes a route secure from different kind of attacks such as reply attack, rushing attack, IP spoofing and man in the middle attack.

Proposed key management is a decentralized and hybrid scheme combining both symmetric and asymmetric cryptographic algorithms; which maintains forward and backward secrecy and provides security against many attacks such as reply attack, man in the middle attack etc. Limitation of proposed key management system and routing protocol is that both use public key cryptography for key sharing and digital signature, which consumes more battery power in comparison of symmetric key cryptography.

REFERECES

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp: 24–30, 1999.

[2]Meng Ge, Kwok-yan Lam, "Self-healing Key Management Service for Mobile Ad Hoc Networks", Proceeding of first International Conference on Ubiquitous and Future Networks", June, 2009.

[3] S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad hoc networks," 2nd Annual PKI Research Workshop (PKI 03), 2003.

[4] H. Y. Luo, J. J. Kong, P. Zerfos, S. W. Lu, and L. X. Zhang, "Ursa: Ubiquitous and robust access control for mobile ad hoc networks, " IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp: 1049–1063, 2004.

[5] Mhd. Al-Shurman, Seong-Moo, Yoo, Bonam Kim, "Distributive Key Management for Mobile Ad Hoc Networks", International Conference on Multimedia and Ubiquitous Engineering, pp: 533-536, 2008.

[6] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37, pp: 29-36 , February 2008.

[7] R. Blom, "Optimal class of symmetric key generation systems", Proceeding of the EUROCRYPT 84 workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, pp: 335-338, December 1985, Paris, France.

[8] H. Nam Nguyen, H. Morino, "A Key Management Scheme for Mobile Ad hoc Networks Based on Threshold Cryptography for Providing Fast Authentication and Low Signaling Load", EUC Workshops-2005, LNCS 3823, pp: 905-915, 2005.

[9] Zhu Lina, Zhang Yi, Feng Li, "Distributed Key Management in Ad hoc Network based on Mobile Agent", Proceeding of 2nd IEEE International Symposium on Intelligent Information Technology Application, vol. 1, pp: 600-604, 2008.

[10] G. A. Safdar, C. McGrath, M. McLoone, "Limitations of Existing Wireless Networks Authentication and Key Management Techniques for MANETs", Proceeding of 7th IEEE International Symposium on Computer Networks, pp: 101-107, 2006.

[11] Yang Ya-Tao, Zeng Ping, and Fang Yong, Chi Ya-Ping., "A Feasible Key Management Scheme in Ad hoc Network", Proceeding of 8th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp: 300–303, 2007.

[12] Azzendine Boukerche and Yonglin Ren, "The Design of a Secure Key Management System for Mobile Ad Hoc Networks", The 33rd IEEE Conference on Local Computer Networks, pp: 302-327, October, 2008.

[13] Xukai Zou, Byrav Ramamurthy, "A Simple Group Diffie-Hellman Key Agreement Protocol without Member Serialization", Computational and Information Science, LNCS-3314, pp: 725-731, 2004.

[14] W. Huang, Y. Xiong, and D. Chen, "DAAODV: A Secure Ad hoc Routing Protocol based on Direct Anonymous Attestation", Proceeding of International Conference on Computational Science and Engineering, August, vol-2, pp: 809-816, 2009.

[15] D. Cerri and A. Ghioni, "Securing AODV: The A-SAODV Securing Routing Prototype", IEEE Communication Magazine: Security in Mobile Ad hoc and Sensor Networks, vol-46, pp: 120-125, February, 2008.

[16] P. Papadimitratos, and Z. Haas, "Secure Routing for Mobile Ad hoc Networks", Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation, January, 2002.

[17] Y.C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks", Proceeding of 8th Annual International Conference on Mobile Computing and Networking, (MobiCom 02), September 2002, pp: 12-23,.

[18] J. Liu, F. Fu, J. Xiao and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks", Proceeding of 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, vol-3, 2007, pp: 314-318.

[19] L. Buttyan, and I. Vajda, "Towards Provable Security for Ad hoc Routing Protocols", Proceeding of 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, October 2005, pp: 94-105.

[20] G. Ács, L. Buttyán, and I. Vajda, "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol-5, November 2006, pp: 1533-1546.

[21] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37, February 2008, pp: 29-36.

[22] Y.Chun Hu, A. Perrig and David B. Johnson, "Wormhole Attack in Wireless Networks", IEEE Journal on Selected Areas in Communication, vol. 24, February 2006, pp: 370-380.

[23] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad hoc Networks", International Symposium on High

Capacity Optical Networks and Enabling Technologies, November 2007, pp: 1-6.

[24] A. K. Shukla, N. Tyagi, "A New Route Maintenance in Dynamic Source Routing Protocol", IEEE International Symposium on Wireless Pervasive Computing, January, 2006.

[25] Q. Niu, "Secure On-Demand Source Routing for Ad hoc Networks", Proceeding of IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 08), October, 2008, pp: 1-4.

[26] Du Congwei, Li Rongsen and Dou Wenhua, "An Efficient Key Agreement Protocol in Cluster-Based MANETs", IEEE International Conference on Computer Application and System Modeling, Taiyuan, China, October 22-24, 2010, vol-10, pp: v10-627-v10-630.

[27] Xie Hai-tao, "A Cluster-Based Key Management Scheme for MANET", Proceeding of IEEE 3rd International Workshop on Intelligent System and Application, May 28-29, 2011, Wuhan, China, pp:1-4.