ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Session Based Access Control Mechanism Using ECC in WMN- A Review

Rahul V.Bambodkar, Avinash P. Wadhe

Assistant Professor, Dept. of CSE, DMIETR, Wardha, India

Assistant Professor, Dept. of CSE, G. H. Raisoni College of Engineering, Amravati, India

ABSTRACT: Wireless Mesh Networks (WMNs) are new emerging potential for strengthening Internet deployment and access. However, for large-scale deployment in some applications due to the lack of the satisfactory guarantees on security. The main challenges exposed to the security of WMNs come from the facts of the shared nature of the wireless architecture and the lack of globally trusted central authorities. A well-performed security framework for WMNs will contribute to network survivability and strongly support the network growth. A low-computational and scalable key management model for WMNs is to guarantee well-performed key management services and protection from unauthorized access. The RSA-based protocols have significant problems in terms of the bandwidth and storage requirements. Currently, the RSA algorithm requires that the key length be at least 1024 bits for long term security, however, it seems that 160 bits are sufficient for elliptic curve cryptographic functions. Thus, use of ECC in wireless mesh network ,can improved security substantially.

KEYWORDS: Wireless Mesh Networks, Security, Key Management, ECC, Diffie–Hellman.

I. INTRODUCTION

Wireless mesh networks (WMN) are multi-radio, multi-hop networks with the ability of dynamically self organizing and self configuring. They can automatically establish ad hoc networks and maintain mesh connectivity between them. They are envisioned to be compatible and interoperable with existing wire line and wireless networks (conventional wireless, cellular networks, sensor networks) through gateways.

WMN's diversify the abilities of ad hoc networks as they are composed of mesh routers and mesh clients. Mesh clients exhibit pure ad hoc behaviour by performing routing and self configuration. The mesh routers are the main addition, on top of providing a mesh of self-configuring and self-healing Links among themselves, they also provide a gateway functionality which enables integration with existing wireless and wire line networks. A mesh router also contains additional routing functions to support mesh networking. A wireless mesh router should be able to achieve the same coverage compared to a conventional wireless router but with lower transmission power..

Hence, even though they exhibit ad hoc behaviour, they still have a network architecture associated; this can be manipulated when looking towards intrusion detection techniques. There are primarily three networks Architectures associated with wireless mesh networks. There is the infrastructure or backbone architecture which is solely composed of mesh routers. This is considered as backbone architecture as it provides infrastructure to wired and wireless clients. This allows integration of mesh networks with already existing communication networks. The second architecture considered is the client wireless mesh network architecture which is comprised of mesh clients that provide peer to peer networks among client devices.

The main difference between mesh clients and mesh routers is that clients only have one wireless interface and less computational abilities. Finally the hybrid architecture is composed of the backbone and client meshing architectures. This way, the infrastructure provides connectivity to other networks and the routing abilities of clients provide improved connectivity and coverage within the mesh network. WMNs consist of two kinds of nodes: mesh routers and mesh clients.

Mesh routers are routers which forms the stationary or least mobile part of the mesh network with less power constraint and forms the backbone of the mesh network. Mesh clients are nodes which are mobile in the network with power constraints. Though mesh clients can also do routing by forwarding packets to the next node in mesh networking the hardware and software platform for them are much simpler compared to mesh routers. Mesh routers can do all the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

gateway/bridge functions as in conventional wireless router, in addition to that it contains additional functions to support mesh routing. They can support multiple wireless interfaces built on either the same or different wireless access technologies.

Thus mesh routers are dedicated and stationary nodes for routing functions with less power constraint. Mesh clients are nodes with no gateway/bridge functions and only one wireless interface is needed in mesh clients. Wireless mesh networks can be integrated with other networks because of the bridge/gateway functions provided by the mesh router. The presence of mesh routers and hop by hop forwarding in WMNs bring many advantages compared to conventional ad-hoc network such as low up-front cost, higher scalability, easy network maintenance, robustness, reliable and need less transmission power. A wireless mesh network enables ad-hoc mode peer to peer interconnection among mesh clients are is called client meshing. With client meshing, mesh routers that stay outside the radio coverage of a mesh router can rely on other intermediate clients to relay packets to them to get WMN access network connections. Thus packets from a mesh client which lies far away from the mesh router has to travel multi hop client-to-client and client-to-router wireless link before reaching its destination. The number of hops is determined by the geographical location of the client and also the organization structure of the access network.

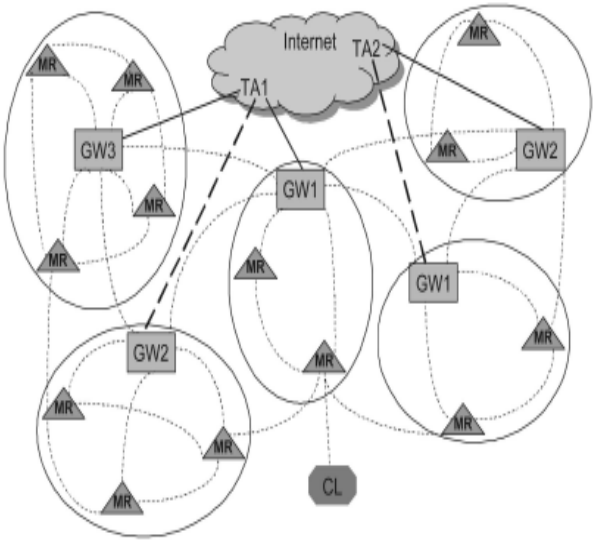


Fig.1: Network topology of typical WMN.

The architecture of wireless mesh networks can be classified in to three main groups based on the functionalities of the nodes namely infrastructure/backbone WMNs, client WMNs and Hybrid WMNs. In infrastructure WMNs wireless mesh routers will form a mesh of self-configuring, self healing links among themselves. With gateway functionality these routers can be connected to the internet. This approach provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers.

In client meshing the client devices will form a mesh to perform routing and configuration functionalities as well as providing end-user applications to users. In this architecture no mesh routers are present and thus are same as the conventional ad-hoc network. Hybrid WMNs is the combination of infrastructure and client meshing and a mesh network is formed between the clients and as well as the routers. Mesh clients can access the network through mesh routers as well as directly meshing with each other. Because of the self configurable architecture of wireless mesh networks and the wide usage of WMNs for accessing internet, mesh routers and clients are prone to different type of security issues.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

So providing solution to the security challenges is a major research area in recent years in the fields of WMNs. WMNs are facing two broad categories of attacks such as passive attacks and active attacks of passive attack, the attackers simply analyse and listen to the network traffic with the objective of capturing sensitive information which can be used later to launch an active attack on the network. Active attacks are which will directly damage the network bandwidth either by tampering, modification or just by dropping of packets. Because of the multi hop nature and ad-hoc connectivity, WMNs are prone to both kinds of these attacks.

The three important features of a secure network are confidentiality, integrity and service availability. Confidentiality is compromised by passive attacks, integrity by active attacks and availability by the most severe form of active attack on internet namely Denial of Service (DoS) attacks and various layer attacks.

LAYER	ATTACK
Aplication Layer	Repudition, data corruption
Transport Layer	Session hijacking,SYN flooding
Network Layer	Wormhole, blackhole, Byzantine, Flooding, resource consumption, location disclosure attack.
Data Link Layer	Traffic analysis, monitoring, disruption MAC(802.11) WEP weakness
Physical Layer	Jamming,interception,eavesdropping
Multilayer	DoS, impersonation, replay, man-in-the middle

Table 1: Comparison of Attack

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants.

ECC has attracted much attention as the security solutions for wireless networks due to the small key size and low computational overhead. For example, 160- bit ECC offers the comparable security to 1024-bit RSA. An elliptic curve over a finite field GF (a Galois Field of order q) is composed of a finite group of points (xi, yi), where integer coordinates xi, yi satisfy the long Weierstrass form:

$$y2 + a1xy + a3y = x3 + a2x2 + a4x + a6$$

ECC-based access control:

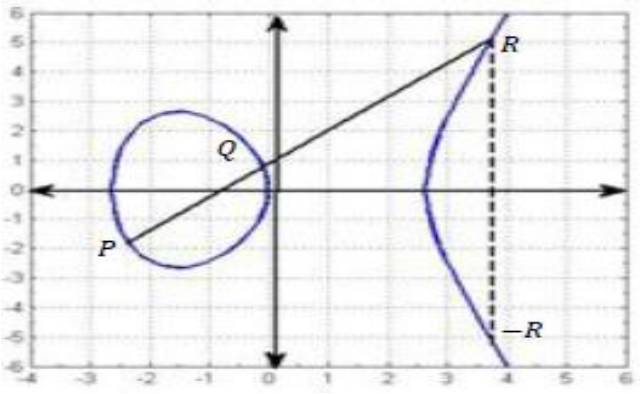
An elliptic curve consists of the points satisfying the equation: $y^2=x^3+ax+b$. Where x, y, a and b are elements in GF (q) (a Galois Field of order, where is a prime).Each choice of (a, b) yields a different elliptic curve. For example, Figure 2 shows an elliptic curve of $y^2 = x^3+7x$, P (-2.35,-186), Q (-0.1, 0.836),-R (3.89,-5.62),P+Q=R= (3.89,-5.62),$y^2 = x^3+7x$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015



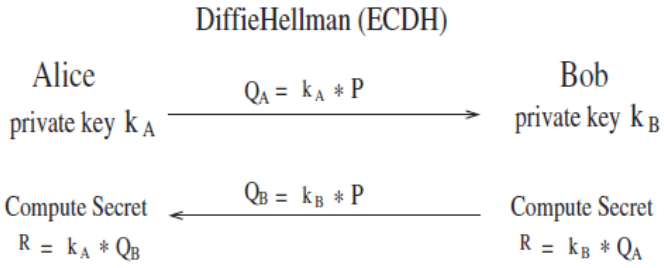
, Figure 2: Elliptic curve of $y^2 = x^3+7x$

And the coefficients are elements in GF (q). Since the field GF (q) (q is a prime) is generally used in cryptographic applications, (1) can be simplified to: y2 = x3 + ax2 + b (2) where a, b ∈ GF(q).The elliptic curve group operation is closed so that the addition of any two points is a point in the group. Given two points P and Q, with the coordinates (x1, y1), (x2, y2), respectively, the addition results in a point R on the curve with coordinate (x3, y3), where x3 and y3 satisfy (x1, y1) + (x2, y2) = (x3, y3) such that x3 = L2 + L + x1 + x2 + a, y3 = L(x1 + x3) + x3 + y1 where L = (y1 + y2)/(x1 + x2).

If x1 = x2 (note x1 + x2 is 0), then R is defined as a point at infinity, O. O is an identity element of the group. Each element in the group has an inverse that satisfies P +(−P) = O and (−P) + P = O. Also, P + O = O + P = P.If P = Q, then R = P + P = 2P, and coordinate (x3, y3) is derived by x3 = L2 + L + a, $y3 = x1+2 + (L + 1)x3$ where $L== x1 + y1/x1$. The ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem, that is, given points P and Q in the group, it is hard to find a number k such that Q = kP .

The original Diffie-Hellman secret sharing protocol (Diffie and Hellman, 1976) requires a key of at least 1024 bits to achieve sufficient security. Unfortunately, low-power architecture, such as MSP430 andATMega128, cannot afford the large memory overhead. Diffie–Hellman scheme based on ECC, however, can achieve the same security level with only 160 bit key size. A typical Elliptic Curve Diffie–Hellman (ECDH) scheme is shown in Figure 1. Initially, Alice and Bob agree on system base point P and generate their own public key QA and QB. To share a secret, Alice and Bob exchange their public keys and then use their own private key to multiply the other's public key. The result point R will be the secret. Eve, an eavesdropper, may overhear the communication and learn the public keys from Alice and Bob. However, with the knowledge of PQA and QB, it is computationally intractable for Eve to get Alice and Bob's private keys. As a result, she cannot figure out secret R.

An example of ECC version of Diffie-Hellman Protocol



ECC can also be used for Digital Signature Algorithm. Similarly, Alice and Bob have to agree on a particular curve with base point P.We assume the field is GF(p) and the order of P is q. When Alice sends a message to Bob, she attaches a digital signature (r, s) generated by following steps (suppose Alice has a private key x and a public key Q = xP):

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

1. Choose a random key k in [1, q − 1]
2. Compute kP , results a point with coordinate (x1,y1).
   Let r = x1. Check r (mod q), go back to the first step if the result is zero.
3. Compute k −1 (mod q).
4. Compute s = k−1(Hash(m) + xr), where Hash is an one-way hash function. Again, check s, go back to the first step if s = 0 and
5. (r, s) is the digital signature.

To verify the message m and the signature, Bob needs to do following steps.

1. Compute w = s −1 mod q and H(m)
2. Compute u1 = H(m)w mod q and u2 = rw mod q
3. Compute u1P + u2Q, get the result point (x2, y2) and
4. The signature is verified if x2 = r.

II. RELATED WORK

Fahad T. Bin Muhaya, Fazl-e-Hadi, AtifNaseer [2] worked on selfish node detection in WNN. The network always faces different types of security attacks by external and internal intruders. Most of the time these intruders are the internal legitimate nodes of the network that behave abnormally and network becomes unsecure. They proposed a novel secure routing approach that identifies the internal intruders in the network using field base routing algorithm. All the nodes in the network have assigned a certificate through mutual exchange from the certification authority (gateway) that makes the node authentic and reliable. Any node in the network can behave abnormally and act as an intruder by advertising its field value to maximum, so all the traffic will divert to those selfish nodes. Every node calculates its field value from their neighbors every node in the network has the information about their neighbor's field value. The node always forwards the packet having highest field value and hence the packet reaches to its destination.

Yatao Yang Ping Zeng Xinghua Yang Yina Huang [3] developed efficient intrusion detection system on proxy based scheme. Proxy analyzes and detects the data characteristics, then can get initiative judgment result. Proxy supervises and analyzes the data by using of Anomaly Detection Method (ADM) or Misuse Detection Method (MDM), the detection result will also be reanalyzed. Central console makes several decisions based on the comprehensive analysis on alarm information. when it is the legitimate user request, the information will be returned and central console enters the safe mode, if the illegal users, central console will produce the alarm report or cut off the wireless communication connection; When Decision Making Module in central console still cannot assure whether the invasion occurred or not, it will require the Secure Communications Module in central console to send data package to other adjacent proxy nodes to carry out the further testing.

ZHAI Min, HUANG Ting-Ieicode [5] proposed Public key infrastructure and Certificate authority (CA) which are two very important authentication mechanisms. Because the wireless mesh network does not have pre-established trusted network architecture, therefore, it is unrealistic to establish a central centralized CA.Many scholars have studied and discussed on this issue and advanced many schemes for establishing a distributed CA and key management algorithm based on threshold Cryptography theory, which is used to build distributed CA. and selection standards that are selecting physically and relatively safe nodes and high calculation ability ones as service nodes. fully distributed CA key management methods, that is, all nodes in the network is provided as a service node with a sub private key to achieve the functionality of the CA. The above schemes have in common is that they need a trusted CA system to divide private key into several copies and to respectively distribute the copies to service nodes, and then to build a virtual CA. These types of partial or full distributed CA scheme are applicable in some areas and industries that having set up a dedicated key generation and management departments. In the above scenarios, a problem encountered is that when the set of service nodes changes, off-line CA must re-distribute the sub-secrets, because the existing sub-secret of the former nodes will be a security risk. However, it is not easy for off-line CA to frequently re-distribute all the sub-secret of services nodes on account of heavy workload.

Some scholars have researched on the questions system calls form I the set of normal patterns for the database, and abnormal sequences indicate anomalies in the running process. M.Imani, M.E.Rajabi, M. Taheri, M.Naderi [6] proposed the Vulnerabilities in network layer. The various Vulnerabilities are: Selective forwarding and Black hole

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

attack, Sinkhole attack, Sybil attack, Wormhole attack, Rushing attack. As all of the wireless networks suffer from much vulnerability. Because the vulnerabilities on network layer have vast effects that can spread their corruption on entire network, these vulnerabilities are very important. The attacker abuse these vulnerabilities to invade the network and these attackers can be from inside or outside the network. The efficient method for preventing external attacker is cryptography with a globally shared key.

Andreas Noack, Jorg Schwenk [7] proposed the application of group key agreement (GKA) protocols. They compare the performance of three group key agreement protocols in new model: Burmester-Desmedt I (BD1), Burmester-Desmedt II (BD2) and the Tree Based Key Agreement (TBKA) protocol. All of the chosen protocols support any positive number of mesh nodes greater than one. Under a cryptographic perspective, there are some slight differences in the security properties of the mentioned protocols, as BD1 and TBKA have contributiveness, whereas BD2 has not. Due to this property, BD2 adapts very good for dynamic groups with continuously joining and leaving nodes. The compared protocols differ in their logical structure. BD1 uses a ring structure which might not be optimal for practical scenarios, where the nodes are normally arranged in a more random order. The logical BD2 structure is a (binary) tree structure without root node, which fits very well in random graphs TBKA, in contradiction to the BD protocols, does not use a fixed logical structure, but demands a particular behavior from the neighbor finding algorithm. Logical neighbors are chosen from the set of direct physical neighbors which works excellent with random graphs. Since a common encryption key in the network will remove the need for re-encryptions and enables a better performance.

III. PROPOSED KEY MANAGEMENT MODEL

To achieve the objective of developing a low-computational and scalable key management for WMNs, this proposed model will be carried out in the following steps:

A. THEORETICAL FRAMEWORK

The theoretical framework would be designed to accommodate Attack Models and Key Management Models. In the Attack Models part, the project will start with some most well-defined and important attacks including eavesdropping (the most common passive attack), DoS (Denial of Services) and replaying attack (two most common active attacks). The defined attack models would be used to analyze the security level of the proposed key management schemes, that is, if the proposed schemes coped well corresponding to the attack models, then high level of security is achieved.[11,12] If possible, more attacks will be measured in order to strengthen the security level of proposed key management schemes. Some new definitions and parameters should be developed in the system initialization stage and some innovative features should be added to the common cryptographic methods to accommodate the Mesh environment. Definitions of node "joining", "leaving", "low-computation", and "scalability" would be given to address the WMN environment at this stage as well.

B. KEY MANAGEMENT MODEL

At this step, the network model and the system setup would be clarified. Three levels of key management schemes would be targeted including key management protocols for (1) Mesh routers (RR) pattern, for (2) Mesh clients (CC) pattern, and for (3) Mesh router and Mesh clients (RC) pattern addressing the different status of entities within WMNs.

• RR Pattern: because the mesh routers form the backbone for the entire networking and have reasonable high input/output capability, highest level of security is required. Additional, the RR model has the good tolerance of computation overhead and most routers are static making the Trusted Third Party (CA) possible. Thus, complicated cryptographic methods, such as PKI, two-party and n-party Diffie-Hellman schemes, can be used to design the key management schemes for RR pattern.

• CC Pattern: because the mesh clients are usually mobile and form the lower layer of communication with low input/output capability, low computation is the most challenging feature and reasonable level of security is required. Thus, in order to design the key management schemes for CC model, some low-computational cryptographic methods, such as symmetric cryptography and threshold secret sharing schemes can be used to host the unique system requirement.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

• RC Pattern: the key management schemes for the Mesh router and Mesh clients (RC) pattern can be in between.In addition, since these three patterns belong to group communication models, the existing results for group key management can be a great help to accomplish the development of key management schemes for the above three patterns. Furthermore, for each pattern, key management approaches, saying key distribution, key transport, key agreement and key updating, would be developed in order to fulfill the whole process and functions of key management services. As mentioned before, the well-defined distributed CA scheme is the bridge in utilizing the existing key management schemes into WMNs.

C. Security Analysis and Performance Analysis

The theoretical proof, security analysis and performance analysis for the proposed key management schemes will be done at this step. Two common tools can be used for the simulation at this stage, MatLab, which is a powerful tool in the numerical computing area and NS-2, which is popularly used in the routing and multi-cast protocols. First of all, the mathematical proof would be done to check the proposed schemes with aims of having general security features, saying confidentiality, integrity [13, 14] and availability, and coping well against the defined attack models to ensure the high level of security. Then by using Matlab, implementation would be carried out to measure the communication and computation costs with the aims of being low-computational. Scalability will be simulated to ensure the proposed key management schemes can cope well with the large extendable networks. At the end, advantages and disadvantages analysis would be provided to evaluate the developed key management model.

IV. Conclusion and Future Work

With more and more applications coming out, the destination of this promising technology, saying WMNs, will be well-performed, secure, and wide-spread wireless connection. ECC-based access control scheme in wireless mesh network the protocol for the network to authorize a user to access the network. Implementation of ECC on primary field performance will increase substantially; in future it is possible to further reduce the running time by using more refined and careful programming. Public-key cryptography is feasible for wireless mesh network security applications including access control.

References

1. Fahad T. Bin Muhaya,King Saud University Fazl-e-Hadi Atif Naseer,'Selfish Node Detection in Wireless Mesh Networks',.International Conference on Networking and Information Technology (ICNIT), pp.284-288, 2010.
2. Yatao Yang Ping Zeng Xinghua Yang Yina Huang,'Efficient Intrusion Detection System Model in Wireless Mesh Network', Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp.393-396, 2010.
3. Jinyuan Sun, Chi Zhang(2011), 'SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks', IEEE transactions on dependable and secure computing, vol. 8, no. 2, pp.295-307,2010.
4. ZHAI Min, HUANG Ting-lei (2010), 'A RSA Keys Sharing Scheme based on Dynamic Threshold Secret Sharing Algorithm for WMNs', International Conference on Intelligent Computing and Integrated Systems (ICISS), pp.160-163,2010.
5. M.Imani Bing He, S M.E.Rajabi M.Naderi , 'Vulnerabilities in network layer at Wireless Mesh Networks (WMNs)', International Conference on Educational and Network Technology (ICENT), pp.487-492,2010.
6. Bing He, Saugat Joshi, Dharma P. Agrawal, 'Group Key Agreement Performance in Wireless Mesh Networks', 35th Annual IEEE Conference on Local Computer Networks(LCN), pp.176-179,2010.
7. Haodong Wang, Bo Sheng and Qun Li, 'Elliptic curve cryptography-based access control in sensor networks', International Journal of Security and Networks, Vol. 1, Nos. 3/4, pp.127-137,2006.
8. ANSI X9.63,'Elliptic Curve Key Agreement and Key Transport Protocols", American Bankers Association, 1999.
9. F. Li, X. Xin and Y. Hu, 'Key management in ad hoc networks using self-certified public key system', International Journal of Mobile Communications, Vol. 5,Issue 1, pp. 94-106,2007.
10. S Mittra, 'A framework for scalable secure multicasting', Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures and protocols for computer communication, Vol. 27,Issue 4, pp.14-18, 1997.
11. F Lee and S. Shieh, 'Scalable and Lightweight Key Distribution for Secure Group Communications', International Journal of Network Management, Vol.14, Issue 3, pp.167-176,2004.
12. H. Mu and Y. Liu, 'Mesh Based Multicast Key Management Scheme in Ad Hoc Networks', 8th International Conference on Signal Processing, Vol.4, Issue 3, pp.126-134,2006.
13. Y. Fu, J. He, R. Wang and G. Li, 'A key-chain-based keying scheme for many-to-many secure group communication', ACM Transactions on Information and System Security (TISSEC), Vol. 7, Issue 4, pp. 523-552,2004.
14. M S. Siddiqui, and C. S. Hong, 'Security Issues in Wireless Mesh Networks', International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp.717-722,2007.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

BIOGRAPHY

Rahul V.Bambodkar is a Assistant Professor in the Computer Science & Engineering Department, Datta Meghe Institute Of Engineering Technology & Research, Sawanghi Meghe, Wardha. He received B.E.(IT) degree in 2009 from SGBAU, Amravati, MS, India. His research interests are Computer TOC (Theory Of Computation), LP(Language Processors), etc.

.**Avinash P. Wadhe** is a Assistant Professor in the Computer Science & Engineering Department, G. H. Raisoni College of Engineering, Anjangao Bari Road, Amravati. He received Master Of Engineering (CSE) degree in 2007 from SGBAU, Amravati, MS, India. His research interests are Computer Networks (wireless Networks), Cyber Forensics, Cyber Crime, TOC (Theory of Computation), etc.