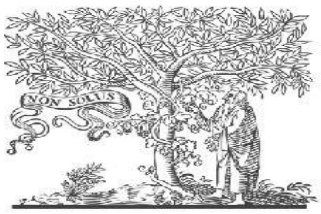
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 15th Nov 2021. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-11

DOI: 10.48047/IJIEMR/V10/I11/10

Title **Secure Data Transmission for Cluster Based Internet Integrated with MANETs**

Volume 10, Issue 11, Pages: 59-65

Paper Authors
Dr. Syed Raziuddin, Mr. Altaf. C, Mr. Shaik Yasar Ahmed, Dr. C. Atheeq

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Secure Data Transmission for Cluster Based Internet Integrated with MANETs

[1]Dr. Syed Raziuddin, [2]Mr. Altaf. C, [3]Mr. Shaik Yasar Ahmed, [4]Dr. C. Atheeq

[1]Professors, Deccan College of Engineering and Technology, Hyderabad, Telangana.
[2]Assistant Professor, Lords Institute of Engineering and Technology, Hyderabad, Telangana.
[3]Assistant Professor, Deccan College of Engineering and Technology, Hyderabad, Telangana.
[4]Associate Professor, Deccan College of Engineering and Technology, Hyderabad, Telangana.

Abstract:

Integrating the Mobile Ad-Hoc Network (MANET) with Internet has many advantages. The Data collected from the Mobile nodes can be broadcasted to the world by connecting the Internet to it via Gateway. Clustering is a practical way to enhance the system performance. Security is a significant issue in the Integrated MANET-Internet climate in light of the fact that in this climate we need to think about the assaults on Internet availability. So, to overcome this issue, we have proposed Secure and Authenticated routing protocol (SARP) to enhance security performance of the networks. This routing protocol is used to discover a secure route and to transmit data packets securely. In this protocol clusters are formed and security relies on the hardness of the symmetric and asymmetric key algorithms. We show the practicality of this convention as for the security prerequisites and security investigation against different assaults. The estimations and reproductions are given to show the security of the proposed convention. The outcomes show that, the proposed convention have preferred execution over the current secure conventions for Cluster based Internet Integrated with MANETs, in terms of security.

Key Words: MANET, Clusters, Secure Data Transmission, Secure and Authenticated Routing Protocol, Symmetric and Asymmetric algorithms.

Introduction

The correspondence in versatile impromptu organizations involves two stages, the course revelation and the information transmission. In an unfriendly climate, the two stages are powerless against an assortment of assaults. In the first place, enemies can disturb the course revelation by mimicking the objective, by reacting with old or debased steering data, or by scattering manufactured control traffic. Thusly, aggressors can discourage the engendering of authentic course control traffic and antagonistically impact the topological information on harmless hubs. Be that as it may, foes can likewise upset the information transmission stage and, consequently, bring about huge information misfortune by altering, deceitfully diverting, or in any event, dropping information traffic or infusing produced information bundles. To give extensive security, the two periods of MANET coordinated with web correspondence should be defended. In web coordinated with MANET all hubs are allowed to join and leave the organization, additionally called open organization limit. All halfway hubs between a source and objective partake in directing, additionally called bounce by-jump correspondences. As correspondence media is remote, every hub will get bundles in its remote reach, it is possible that it has been parcels objective or not. Because of these qualities, every hub can undoubtedly access different hubs bundles or infuse issue parcels to the organization. Subsequently, getting MANET against malevolent conduct and hubs became one of the main difficulties in MANET [1]. A MANET is an independent assortment of versatile clients that move subjectively and impart over multi-jump transfers. Internet integrated with MANET is an extension of wireless sensor networks. To establish the connection between the cluster head and Internet integrated with MANET, a gateway is required.

A. Clustering in MANETs

One promising way to deal with address directing issues in MANET conditions is to construct pecking orders among the hubs, to such an extent that the organization geography can be preoccupied. This interaction is generally alluded to as bunching and the bases that are fallen in more elevated levels are called groups [2]. The idea of grouping in MANETs isn't new; numerous calculations that consider various measurements and spotlight on assorted targets have been

proposed [2]. Be that as it may, most existing calculations neglect to ensure stable bunch developments. All the more significantly, they depend on occasional telecom of control messages bringing about expanded utilization of organization traffic and portable hosts energy.

B. MANET Internet Connectivity

As a rule, when a MANET hub needs to send bundles to some decent arrange, it should communicate the parcels to an entryway, since that the door proceeds as a scaffold job between a MANET and the Internet. Thus, it is important to execute every one of the MANET conventions stack and the TCP/IP suite. A versatile Ad Hoc hub runs conventions that have been expected for remote channels, for example, (IEEE 802.11 DCF) in the physical and information interface layer. Initially, in the organization layer, either an IP based Ad Hoc directing convention, e.g., Ad Hoc On Demand Distance Vector Routing (AODV) convention [3] is utilized, or this layer might be isolated into two sub layers, called the typical IP layer over an on IP based Ad Hoc steering convention that moves the IP parcels in the promotion network utilizing an exemplified way. Door incorporates conventions of both the wired Internet and the remote Ad Hoc organization. On the Internet side, it utilizes the commonplace Internet conventions. In any case, on the Ad Hoc side, it sends and gets parcels by an Ad Hoc directing calculation. At long last versatility the board is accomplished by utilizing Mobile Internet Protocol [3]. The Internet entryway gives us a figment that the MANET is in effect a typical IP subnet.

C. Attacks on Internet MANET Integration

1) Attacks on Gateway

1.1 Fake Registration: A counterfeit enrollment is a functioning assault where an assailant does an enlistment with a false consideration of address by imagining itself as another person. Presently, the aggressor can catch touchy individual or organization information to get to arrange and may upset the appropriate working of organization. It is hard for an assailant to carry out such sort of assault on the grounds that the aggressor probably point by point data about the specialist [4].

1.2 ***Replay Attack***: A replay assault is a type of organization assault in which a legitimate information transmission is vindictively or falsely rehashed or deferred. This is done either by the originator or by a the enemy information and retransmits it.

2) Attacks on internet

There are two sorts of assaults inactive and dynamic. The uninvolved assault doesn't change information parcels or adjust any tasks for control bundles. It is simply caught to the parcels during transmission without adjust them. An assailant requires being inside radio scope of a hub to tuning in. Here the assault points the privately necessity. The finding of this assault is truly challenging because of it isn't evolving anything. One answer for this assault is to utilize strong encryption techniques to scramble the information need to communicate. In dynamic assault, the enemy hub intercedes against the activities of the organization. This assault can influence the organization directing way, perusing either by modifying the steering information, bounce count, caricaturing another hub IP and other. While in the forward bundle, this assault is done either by drop the parcel, perusing and changing the bundles. The recognition of dynamic assault is simple since it made some modification to the organization work [5].

2.1 Active assaults: The names of some dynamic assaults are Spoofing, Fabrication, Wormhole assault, Denial of administrations assault, Sinkhole assault, and Sybil assault.

2.2 Passive assaults: The name of some uninvolved assaults is Eavesdropping, traffic investigation, and Monitoring.

The remainder of this paper is organized as follows. Section 2 describes the security requirements. Section 3 describes the related work. Section 4 describes the system architecture. Section 5 presents the details of the proposed protocol Section 6 presents the Simulation results. The last section concludes this work.

II. SECURITY REQUIREMENTS

The security prerequisites indicated underneath determined by International Telecommunications Union (ITU-T) addressed in their proposal X.805 and X.800 [6]:

Authentication: Authentication is fundamental to check the character of each hub in MANET and its qualification to get to the organization. This implies that, hubs in MANETs are needed to confirm the characters of the conveyed substances in the organization, to ensure that these hubs are speaking with the right element.

Authorisation and Access Control: Each hub in MANET is needed to have the admittance to shared assets, administrations and individual data on the organization. Likewise, hubs ought to be fit for confining each other from getting to their private data. There are numerous strategies that can be utilized for access control like Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC).

Privacy and privacy: Each hub needs to get both the data that is traded between one another; and secure the area data and the information put away on these hubs. Security implies forestalling the character and the area of the hubs from being uncovered to some other substances, while privacy implies holding the mystery of the traded information back from being uncovered to the individuals who have not authorization to get to it.

Availability and survivability: The organization administrations and applications in MANET ought to be available, when required, even within the sight of issues or malignant assault, for example, forswearing of administration assault (DoS). While survivability implies the capacity of the organization to reestablish its ordinary administrations under such these conditions. These two prerequisites ought to be upheld in MANET.

Data uprightness: The information sent between hubs in MANET ought to be gotten to the expected elements without been altered or changed by unapproved alteration. This prerequisite is fundamental particularly in military, banking and airplane control frameworks, where information change would make possible harm.

Non-disavowal: This guarantees that hubs in MANET when sending or getting information bundles ought not have the option to reject their obligations of those activities. This necessity is fundamental particularly when debates are researched to decide the got rowdy element. Accordingly advanced mark procedure is utilized to accomplish this necessity to demonstrate that the message was gotten from or sent by the supposed hub.

III. RELATED WORK

For giving security in MANET, the primary destinations are to make the directing convention secure and to ensure communicated information. Be that as it may, these are especially trying for MANETs with powerfully evolving geographies. Following plan is proposed in the writing to get the directing convention and information transmission.

In this section we explore one of the existing secure routing protocol for MANETs i.e. DSR [7] routing protocol. It prevents to enter a malicious node into the path that is established between sources to destination during route discovery methodology using MANET's DSR Routing Protocol. In DSR routing protocol it detects a malicious node and there is no Key generation mechanism. If there is no Key generation then there is no authenticity in the data transmission, so attackers may attack the data which is being transmitted from source and destination. In the proposed protocol we have used key generation mechanism to prevent the malicious node.

Hu et al. [8] have proposed a secure routing protocol based on DSR in which an occurrence of insertion of random delays before forwarding RREQ is a disadvantage whereas in proposed SARP no random delays occurs and route request packets are forwarded continuously.

Secure AODV (SAODV) [9] proposes a bunch of expansions that protected the AODV steering bundles. Two instruments are utilized to get the AODV messages: advanced marks to validate the non-changeable fields of the messages, and hash chains to get the jump count data. Since the convention utilizes topsy-turvy cryptography for computerized marks it requires the presence of a key administration system that empowers a hub to procure and check the public key of different hubs that take an interest in the impromptu organization. In the proposed protocol we have used key generation mechanisms for secure data transmission from mobile source node to fixed destination.

In cluster based security [10, 11, 12] there is no internet connectivity and no cluster head is formed. So in proposed protocol internet connectivity is provided via gateway. In MANET integrated with internet [13, 14] no clusters are formed where as in proposed protocol clusters along with cluster head is formed for secure data transmission.

IV. SYSTEM ARCHITECTURE

Consider a Cluster based MANETs integrated with internet (Fixed Node) via Gateway consisting of huge number of portable hubs, which are homogeneous in

functionalities and capacities. We accept that the Gateway is consistently dependable, i.e., the Gateway is a confided in power (TA).

Fig1MANET integrated with Internet via Gateway

In the mean time, the portable hubs might be undermined by aggressors, and the information transmission might be hindered from assaults on remote channel. In a Cluster based MANETs, versatile hubs are gathered into groups, and each bunch has a portable bunch head (MCH) hub, which is chosen independently. Leaf (non-CH) portable hubs, join a bunch and transmit the data to the Gateway via MCHs to provide security. Then Gateway transmits the data to the fixed node. Also, we expect that, every portable hub and the Gateway are time synchronized with symmetric radio channels, hubs are appropriated haphazardly. In Cluster based MANETs, information detecting, handling and transmission burn-through energy of Mobile hubs.

The expense of information transmission is significantly more costly than that of information handling. In this way, the technique that the halfway hub (e.g., a MCH) totals information and sends it to the proper hub is liked, than the strategy that every portable hub straightforwardly sends information to the decent hub [1, 3]. A versatile hub switches into rest mode for energy saving when it doesn't detect or communicate information, contingent upon the TDMA (time division various access) control utilized for information transmission.

The data is transmitted secure by using Secure and Authenticated routing protocol (SARP). The secure route is discovered before transmitting data and then key management scheme is performed by using symmetric and asymmetric key algorithms. The symmetric key algorithm is performed between gateway and fixed node and asymmetric key algorithm is performed between mobile source node and gateway.

V. Proposed System

In proposed system we are providing secure data transmission in MANETS integrated with internet via gateway. In cluster based MANETs integrated with internet to provide secure transmission of data from mobile nodes to fixed node (Internet) a secure routing protocol is used i.e., Secure and Authenticated routing protocol (SARP) is used, It explains how data is transmitted securely by establishing a secure route between a mobile source nodes and a fixed node (Internet). Multi-hop communication is also performed to transmit data from source mobile node to mobile cluster head.

The security of this proposed protocol relies on the hardness symmetric and asymmetric key algorithm. The key idea of this protocol is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

•SARP is proposed in order to further reduce the computational overhead for security using the Key Management Scheme (KMS), in which security relies on the hardness of the symmetric and asymmetric key algorithm. This protocol solves the orphan node problem in the secure data transmission with a symmetric key management.

•We show the feasibility of this proposed protocol with respect to the security requirements and analysis against various attack models. Moreover, we compare the proposed protocol with the existing secure protocols for efficiency by calculations and simulations respectively, with respect to both computation and communication.

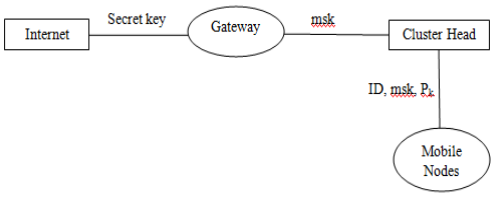


Fig.2 Symmetric and Asymmetric Keys

A. Secure Route Discovery

Secure and Authenticated routing protocol is proposed to secure ad-hoc Internet connectivity as our hybrid gateway is based on DSDV protocol. In the SARP, “cryptographic certificates mechanisms” is used to authenticate the route.

MSN	Mobile source node
IN	Intermediate node
MCH	Mobile Cluster Head
GW	Gateway
FN	Fixed node

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

C	Certificate
IPM	IP address of source node.
REQ_id	Route Request Packet identifier.
REP_id	Reply packet identifier.

Table 1: Variable and Notations

1) Authenticated Route Discovery

Step1: When a way to fixed hub is required, the portable source hub begins a course disclosure process by communicating a course demand bundle (REQ) to its neighbors. Since the parcel is just endorsed by portable source hub and not scrambled, the substance of the bundle is intelligible freely.

Step2: When middle of the road hub gets the REQ parcel sent by source hub, portable group head approves the mark for source hub and sets up a converse way back to source hub by recording the moderate hub from which it got the REP. Then, at that point, middle hub signs the principal field of the got REQ, affixss its own testament, and broadcasts the changed REQ bundle to its group head.

Step3: When getting the sent REQ bundle from transitional hub, portable group head hub approves the marks for both source hub and middle hub utilizing the endorsements in the REQ parcel. Group head then, at that point, eliminates transitional hub's testament and mark, signs the substance of the message initially communicated by source hub and adds its own declaration, and afterward broadcast the new REQ parcel.

Step4: Similarly, door advances the REQ bundle further.

2) Authenticated Route Setup

Step1: When getting the REQ bundle sent by door, the objective, fixed hub, unicast an answer (REP) parcel to passage.

Step2: Gateway signs the REP bundle, adds its own testament, and afterward unicast the parcel to the following bounce towards the source hub.

Step3: Similarly, group head advances the REP parcel further.

Step4: Intermediate Node advances the REP bundle to the source hub.

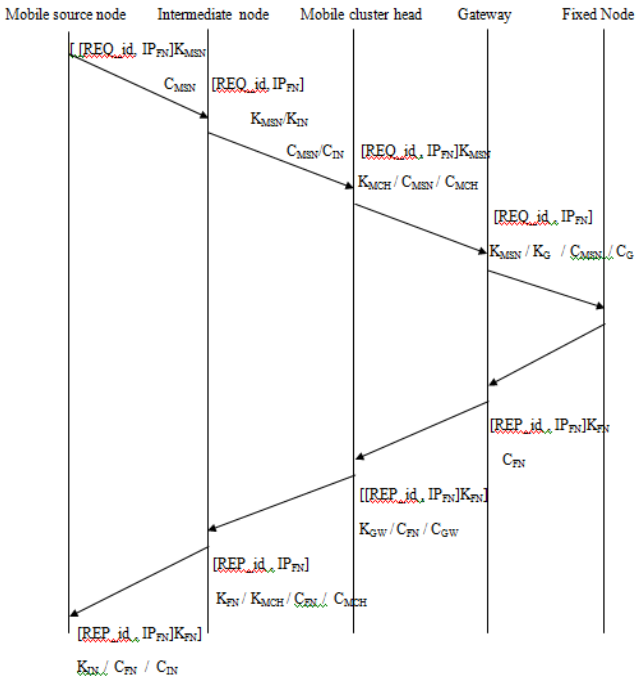


Fig: 3 Process of Authenticated Routing

Till now, a safe way to objective is found. With confirmed course disclosure and validated course arrangement, a source accepts that the hub that starts the comparing verified course arrangement process is without a doubt the expected objective.

3) Authenticated Route Maintenance

To keep up with directing tables, every hub will communicate a steering update parcel to every one of its neighbor switches intermittently. Steering update parcels contain the data from the sender's own directing table

B. Key Management Scheme

1) Asymmetric Key Algorithm

This asymmetric key algorithm here we are using is secure key exchange algorithm comprises of the accompanying tasks, explicitly, arrangement at the Gateway, key extraction and mark marking at the information sending hubs, and check at the information getting hubs.

i. **Setup:** The Gateway (GW) (as a trust authority) produces an expert key msk for the private key generator (PKG), and gives them to all versatile bunch hubs.

ii. **Extraction**: Given an ID string, a versatile hub produces a private key sekID related with the ID utilizing msk.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

iii. **Signature marking**: Given a message M, time-stamp t and a marking key, the sending hub produces a mark SIG.

***iv. Verification*:** Given the *ID*, *M* and *SIG*, the receiving node outputs "accept" if *SIG* is valid, and outputs "reject" otherwise.

2) Symmetric Key Algorithm

In symmetric key algorithm we are using Diffie-Hellman algorithm to share keys between gateway and fixed node.

i. Fixed node and Gateway agree on a prime number p and a base q.
ii. Fixed node chooses a secret number f, and sends Gateway (q^f mod p).
iii. Gateway chooses a secret number g, and sends fixed node (q^g mod p).
iv. Fixed node computes ((q^g mod p)^f mod p).
v. Gateway computes ((g^f mod p)^g mod p).

Both Fixed node and Gateway can use this number as their key. Notice that p and q need not be protected.

VI. Simulation Results

The reenactment results are acquired under a few investigations. The outcomes for proposed work have been contrasted and the aftereffects of SAODV convention utilizing Xgraph. XGRAPH has been utilized to lead subjective examination. The boundaries viable are Packet conveyance proportion and Throughput. The accompanying graphical examination shows the presentation aftereffects of SAODV and SARP conventions. Fig.4. shows the Xgraph for SAODV and SARP with a respite time set to 25ms. The X-hub of the chart demonstrates the No. of Nodes and the Y-hub shows the Packet Delivery Ratio. This chart shows at hub 50 the PDR proportion of SARP is 96.59 % and PDR Ratio of SAODV is 84.62 %. In this figure when the transmission goes from 25th hub to 100th hub. Here the PDR of SARP will increments yet the PDR of SAODV will diminishes .In fig PDR of SAODV diminishes when organization size increments where as PDR of SARP increments when organization size increments since it has less bundle misfortune. SAODV plot gives 80.87% PDR yet SARP conspire furnishes 97.02% PDR in network size with 100 hubs. This fig 5 shows that throughput of SAODV start from 25th hub and it comes to 80% at 100th hub. However, throughputs of SARP will increment when organization size increments. It arrives at most extreme throughput 95% at 100th hub. So SARP gives most elevated throughput than SAODV. Additional directing parcels are created and conveyed by SARP than SAODV.

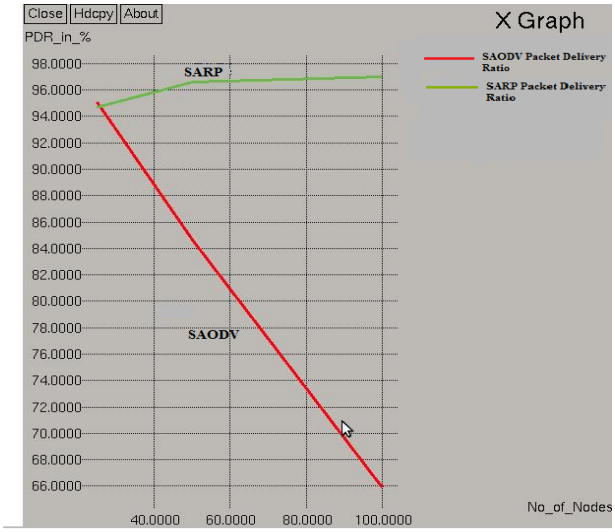


Fig 4. Packet Delivery Ratio

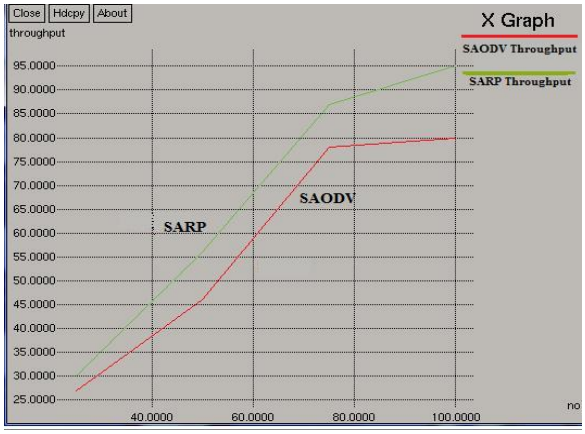


Fig 5. Throughput

VII. Conclusion

This paper has presented a comprehensive review of solutions for integration MANETs with Internet. In this paper, we first reviewed the attacks on Gateway and MANETs. Secure and Authenticated Routing Protocol (SARP) is designed to ensure secure functions. Secure data transmission is provided between mobile source node to fixed node via gateway by using Symmetric and Asymmetric key algorithms. Ultimately, the examination in the estimation and reenactment results show that, the proposed SARP convention have preferable execution over existing secure conventions in Internet integrated with MANETs. In future work instead of using two algorithms, only one algorithm can be used to provide secure data transmission by using an effective and robust protocol. It is normal that it will limit the security assaults because of both coordinated MANET-Internet and remain solitary MANET. The exhibition examination of the convention will be finished utilizing NS-2 reproduction programming.

REFERNCES

[1] ”Strategies and Analysis of Mobile Ad Hoc Network-Integration Solutions”, Rakesh Kumar, Anil K. Sarje and Manoj Misra.

[2] “Cluster Based Security Architecture in Wireless Ad-hoc Networks: An Overview”, Avinash Jethi and Seema.

[3] “Rakesh Kumar. et al, Review Strategies and Analysis of Mobile Ad Hoc NetworkInternet Integration Solutions, International Journal of Computer Science Issues, Vol. 7, Issue 4, IJCSI. No 6, July 2010.

[4] Nishu Garg, R.P.Mahapatra. “MANET Security Issues”. IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2010.

[5] Gagandeep, Aashima, Pawan Kumar,Analysis of Different Security Attacks in MANETs on Protocol Stack a-Review, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[6] Shobha Arya1 And Chandrakala Arya2, “Malicious Nodes Detection In Mobile Ad Hoc Networks”, Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.

[7] Milan Kumar Dholey,G.Biswas,”International Conference on Intelligent Computing,communication &convergence (ICCC-2015).

[8] Milan Kumar Dholey,G.Biswas,”International Conference on Intelligent Computing,communication &convergence (ICCC-2015).

[9] Preeti Sachan and Pabitra Mohan Khilar “Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[10] D. J. Baker and A. Ephremides. The architectural organization of a mobile radio network via a distributed algorithm. IEEE Transactions on Communications, 29(11):1694-1701.

[11] Safa, H.; Artail, H.; Tabet, D.: A cluster-based trust-aware routing protocol for mobile ad hoc networks. J. Wired. Networks. 16, 969--984 (2010).