I.J.Computer Network and Information Security, 2014, 2, 30-37
Published Online January 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.02.05

Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks

M.Madhurya, B.Ananda Krishna, T.Subhashini
Department of ECE, Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt, AP, India
Email: madhurya.honey@gmail.com, anand_bk@rediffmail.com, subhashini.anagani@gmail.com

Abstract—Mobile Ad hoc Networks are wireless infrastructure less networks can be easily formed or deployed due to its simple infrastructure. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. The main objective of this work is to enhance the performance of the network by securing the data and to minimize the malicious nodes which disturb the stream of the network. Securing data is a critical task which can be achieved by cryptographic algorithms and disturbance detection plays as a crucial ingredient in any comprehensive security solution to address the threats. Hence a Novel Cryptographic Algorithm with a new Disturbance Detection System (DDS) has been proposed for Mobile Adhoc Networks. This method prevents the outside attacks to obtain any information from any data exchange in network and also use promiscuous mode of working along with rating and collaborative decision making based on multiple threshold values. The proposed algorithm was implemented and simulated in the Glomosim and the result analysis proved that the performance of the network is increased.

Index Terms—MANET, Network Security, Encryption, Decryption, DDS.

I. INTRODUCTION

An autonomous system which comprises a collection of mobile nodes that use wireless transmission for communication is known as Mobile Ad hoc Networks (MANETs) [1]. They are self-organized, self-configured and self-controlled infrastructure less networks i.e. it has no central controlling authority. These networks are mainly used by community of users such as military, civilian and emergency services. The advantages of MANETs are smaller in size, more convenient, more powerful, support high speed multimedia services, high mobility, device portability and low cost. Limitations that have to be overcome in a MANET environment [2] are securing data, link failures, power consumption and limited transmission range.

The security in the network plays an important role and can be achieved by cryptographic algorithms [3]. Cryptography is the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender to receiver within the network. The cryptographic algorithms are of two types [4] symmetric key and asymmetric key algorithms. Symmetric key algorithm uses single key to encrypt and decrypt the data whereas, asymmetric key algorithm uses two types of keys i.e. public key for the encryption and private key for the decryption. Two important properties of crypto systems are its speed and security. Speed refers to the time taken by the algorithm to convert a given plain text to cipher text. Key plays a prominent role in encryption and decryption algorithm and its size determines the strength of encryption algorithms. The increase in key size reduces the speed of the algorithm but in turn increases the security.

A routing protocol specifies how routers communicate with each other; disseminate information that enables to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. A routing protocol shares this information first among immediate neighbors, and then throughout the network. Routing protocols are used for directing the traffic or data packet from source to the destination may lose the data due to attacks on ad hoc networks [5]. In order to secure data the goals to achieve are availability, confidentiality, integrity, authentication, non-reputation.

There has been appreciable work by research community in message encryption, digital signature,key management, etc., that address the confidentiality of messages in transit over the unsecured medium. Many challenges particularly related to the privacy and data confidentiality, however, remain to be solved. Existing approaches which have been used in MANETs such as access control, digital signature, and encryption focused only in securing the channel during the transmission. However how these nodes act after and use this information has been mostly neglected.

In this paper, we review the main security issues and existing solutions in MANET, particularly in which has not been widely addressed. We present a Novel Cryptographic Algorithm and a new condition based collaborative Disturbance Detection System for mobile ad hoc networks. The purpose of this architecture is to keep the data confidential and to minimize the disturbance occurred due to malicious activity in the route. The disturbance or misbehavior of the each node is detected and intimate to the neighboring nodes is implemented by Disturbance Detection Algorithm (DDA). The nodes collect and analyze data for the entire

network ensuring that the contents of messages are kept secret to an originator defined subset of peers in MANETs.

The paper is organized as follows. SectionII provides the background about types of collaborative disturbance detection systems in MANETs. Related work on Security issues and intrusion detection is discussed in sectionIII. Section IV describes the problem statement. The details of the proposed scenarios based upon the information security with authentication have been discussed in section V. Methodology for the development of the simulation environment using Glomosim to evaluate the effectiveness of the proposed algorithm has been discussed in sectionVI. Based upon the simulation results, conclusions have been drawn and future work has been proposed in sectionVII.

II. TYPES OF COLLABORATIVE DISTURBANCE DETECTION SYSTEMS

Disturbance Detection Algorithm detects the critical node which has malicious behavior that disconnects or significantly degrades the performance of the network. The data packets may be dropped due to network congestion or because of a malicious behavior of a node which doesn't executes a routing algorithm faithfully. Researchers have proposed many collaborative DDS schemes like:

- Neighbor-monitoring
- Trust building
- Cluster-based voting

Examples of disturbances are:

- *Web servers defacement*
- *Guessing/cracking passwords*
- *Remote route compromise*
- *Copying viewing sensitive data/databases*
- *Running a packet sniffer*
- *Distributing pirated software*
- *Using an unsecured modem to access net*
- *Impersonating a user to reset password*
- *Using an unattended workstation*

III. RELATED WORK

The authors ShashiMehrotra Sethet al, [6] proposed a contemporary review of comparative analysis of encryption algorithms like AES, DES andRSA for data communication by using encryption time; memory usages output byte and battery power. Based on text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while the difference in encryption time is very minor in case of AES and DES algorithms. RSA consumes longest encryption time, high memory usage and less output byte.

The authors Pratap Chandra Mandalet al, [7] studied the evaluation of performance of selected symmetric key algorithms. From the simulation they concluded that Blowfish cryptographic algorithm has better performance than other algorithms. Secondly AES gives better performance than DES and 3DES in terms of throughput and decryption time.

The authors Gurjeevan Singhet al, [8] studied throughput analysis of various selected encryption algorithms like DES, AES, 3DES and Blowfish. The simulation results shows the numerous points like Blowfish has better performance than other algorithms followed by AES in terms of throughput and 3DES has least performance than others.

The authors ChhayaNayaket al, [9] studied the performance of selected symmetric encryption algorithms used in cryptography. Security of information in transit is a very important task in secured communication. Many ciphers are available which have been developed by using arithmetic and logical operations. The two important desirable properties of the cryptosystems are its speed and security. The security of the algorithm is based on the key size. The increase in the key size reduces the speed of the algorithm. But in turn increases the security. Thus the aim of the designer is to design efficient cryptosystems with acceptable speed and appreciable security strength with large key length. Implementation procedures also play a major role in cryptosystems design.

The authors Gulshan Kumar et al, [10] studied the implementation of Cipher Block Chaining (CBC) in wireless sensor networks for security enhancement. The capability of generating encrypted packets and battery consumption is efficient using block cipher mode encryption that provides more security, confidentiality, and authentication. As using block cipher encryption it is hard to break the security by intruder as compare to that of stream cipher. Also CBC block cipher mode of operation is most efficient as it effectively scrambles the plain text prior to each encryption steps.

The authors Gurjeet Singh et al, [11] studied the security threats and maintain in mobile ad hoc networks. MANETs present different threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. MANETs are generally more prone to physical security threats than are fixed cable networks. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of the network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

The authors Wenjia Li and Anupam Joshi [12] studied the security issues in MANETs. The main attack types and several security techniques that help the MANETs to protect from internal or external attacks and aspects of intrusion detection are discussed in their survey paper.

The authors Deepinder Singh Wodhwa et al, [13] give the performance comparison of single and multipath routing protocols in ad hoc networks. They have simulated and compared the protocols like AOMDV, AODV and DSDV in different simulation scenarios and observed their behavior in terms of packet delivery ratio, instant jitter and throughput in order to find out which one should be preferred when the MANET has to be setup for the particular duration. They concluded that AOMDV is preferred over AODV and DSDV for packet delivery ratio. The performance of AODV is better than other two protocols as the network size has increased and in terms of throughput all three protocols have almost the same performance. AOMDV performs better than other two routing protocols.

The authors Subash Chandra Mandhataand Dr.Surya Narayan Patro [14] proposed a counter measure to black hole attack on AODV based MANETs. It is one of the active DOS in which malicious node impersonates a destination node by sending a forged RREP to the source node. In this paper they studied the black hole attack by the existence of single malicious node in the network and its solution proposed by various authors. Review of proposed solutions suggests that the performance of the routing protocol is affected in terms of additional overheads, end-to-end delay and packet delivery ratio.

The authors AmandeepKaur et al, [15] proposed trust formalization in MANET within multichannel. This would be helpful in establishing keys in the network and nodes can communicate data securely without any delay in MANETs. Due to this problem like transmission delay, security can be solved to achieve better performance of QOS and throughput. We provide an overview of routing schemes proposed for ad hoc mobile networks. In which make the comparison between AODV and DSR routing protocol performance for transmission.

The authors Adnan Nadeem and Michael P.Howarth [16] proposed a survey of MANET intrusion detection and prevention approaches for network layer attacks. This enables a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities. Protection mechanism needs to robust enough to protect them and not introduce new vulnerabilities into the system.

The authors Yao Yu and Lincong Zhang [17] proposed a secure clustering algorithm in MANETs shows that the algorithm can improve the security of clustering and obtain good performance through rapid detecting, diagnosing and reacting to various invasions.

The authors AmandeepMakkar et al, [18] proposed a behavioral study of MANET routing protocols. In this research paper, an effort has been made to concentrate on the behavioral study and performance analysis of various prominent routing protocols like DSDV, DSR, TORA, and AODV on basis of quantitative and qualitative metrics. Based on performance analysis, recommendations have been made about the significance of either protocol under different circumstances and the analysis concludes that both protocols are good in performance in their own categories.More over due to dynamically changing topology and infra structure less property, secure and power aware routing is hard to achieve in MANETs.

IV. PROBLEM STATEMENT

The main objective of this work is to achieve data confidentiality and authentication by novel cryptographic algorithm and also to secure the routing protocol by minimizing the malicious nodes. The proposed work consists of two sections they are:

A. Implementing a novel cryptographic algorithm which gives the data security with authentication [19].
B. Condition based routing protocol is designed, which offers quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilization.

The security of routing protocol is compromised by various Denial of Service attacks. In these attacks the malicious node advertises as if it has the shortest path to the destination, thereby halting the transmission that reduces the efficiency of the network. To overcome the problem, we proposed a condition based routing protocol that detects and reduces the disturbances which acquires high throughput.

V. PROPOSED WORK

A. Data Encryption and Authentication

In order to have data security, all the data packets are encrypted and decrypted using a private key and authentication can be obtained by asymmetric cryptography [20]. For this we proposed a novel cryptographic algorithm, which combines both the features of symmetric and asymmetric cryptography along with circular rotations that enhances the strength of the algorithm.

Encryption – Plain text is a readable message or data that is fed into the algorithm as input. By performing circular rotation, bits can shift either left or right as per our requirement. Cipher text is a scrambled message produced as output which depends on plain text and the key. In the proposed algorithm we have used two different set of keys in which one set is used for securing plain text and another set is for authentication. The encryption, key generation and decryption process are shown in Figures [1], [2] and [3].

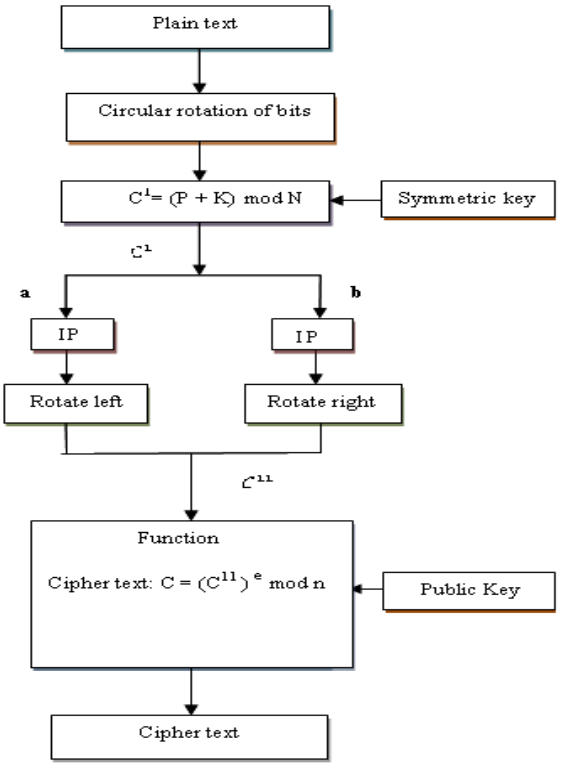

Figure 1: Encryption of plain text

The plain text is circularly rotated either left or right and then encrypted using symmetric key yields cipher text 1 (c^1), which is divided into two equal blocks. An initial permutation (IP) is performed on each block and carries out left and right rotation jointly produces cipher text 2 (c^{11}) as shown in the Fig. 1.

IP
2 6 3 1 4 8 5 7

Then perform the function on c^{11} using asymmetric key which produces the final cipher text. Thus the encryption algorithm ensures data security as well as authentication. The asymmetric keys (public and private) generation is shown in the Fig. 2.

Key generation

Select **p, q**	**p** and **q** both prime, **p ≠ q**
Let **n = p*q**	
Calculate **Φ (n) = (p-1) (q-1)**	
Select integer **'e'**	gcd (**Φ (n), e**) = **1; 1 < e < Φ(n)**
Calculate **'d'**	**d = e** $^{-1}$ **mod Φ (n)**
Public key	KU = **{e, n}**
Private key	KR= **{d, n}**

Figure 2: The key generation algorithm

Decryption – The Fig.3shows decryption algorithm, in which the asymmetric (private) key is generated to decrypt the received cipher text by the decryption function, produces the output c^{11}. The scramble text c^{11} is divided into two blocks 'a' and 'b' and performs rotation of bits reverse to encryption process and perform inverse permutation (IP^{-1}) which results c^1.

IP^{-1}
4 1 3 5 7 2 8 6

Then by using symmetric key, decrypt the text $c^1$and apply circular rotation reverse to encryption process yields the plain text. The key must be the same size of the plain text.

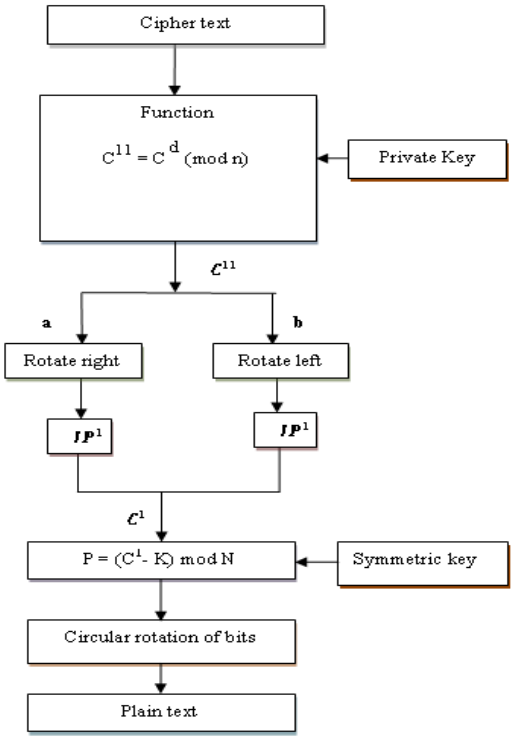

Figure 3: Decryption of cipher text

B. Condition based AODV protocol

The work is extended with the implementation of the condition based AODV protocol to eliminate maliciousness. Our protocol mainly tries to detect and avoid the disturbance in the path. We included an Integrity Rate Index termed as i-rate where in every node is assignedani-rate value of '1' when it enters the network. The i-rate of a node dynamically increases or decreases depending on its behavior. Incentives are given to each node to forward the packets for the other nodes. In contrast, a node is punished if it does some malicious activity like dropping packets, etc., combining the above mechanisms we can detect and avoid the disturbance in the network. The overall process of condition based Disturbance Detection System (DDS) has been illustrated in a flow chart in Fig. 4.

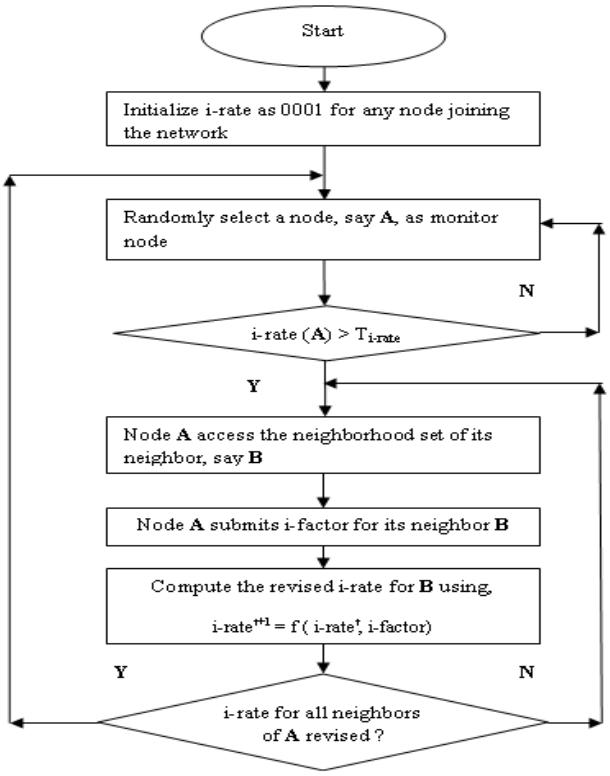

Figure 4: Flowchart for Condition based DDS

The following are the assumptions made in order to design the proposed condition based Disturbance Detection System:

1. In direct wireless transmission range, a node can overhear activity of other nodes in link layer and provide unique identification to every node in the network.

2. For the entire network set the pre-calculated threshold values.

3. All data packets are to be encrypted and signed by the private key of sender using asymmetric key cryptography. This would ensure authenticity and non-repudiation, along with the condition based DDS.

Each node is assigned an integrity rate to signify its trust value, which is represented by a nibble $i_0\ i_1\ i_2\ i_3$. Each new node is initialized with an i-rate of 0001. The integrity rate of a node is dynamically re-assessed and modified by an arbitrary monitor node using conditions. Any packet transmitted will contain the i-rate of the sender. So the receiver can decide what to do with the packet. Thus, any packet of the network in this method will be sent with the following additional fields in the header:

Unique identity of sender	4 bit i-rate

If a node '$\mathbf{K_A}$' has **i-rate** < $\mathbf{T_{i\text{-}rate}}$, then the node can increase it by simply forwarding packets. A threshold value '$\mathbf{T_{GEN}}$', is used to monitor malicious activity, above which a node is not allowed to generate packets. Each node '$\mathbf{K_A}$' in the network stores neighborhood data set '$\mathbf{KS_A}$' in the form of {$\mathbf{K_B}$, $\mathbf{P_{TB}}$, $\mathbf{P_{FB}}$}.

Where, $\mathbf{K_B}$ is a neighbor of $\mathbf{K_A}$.
$\mathbf{P_{TB}}$is the number of packets forwarded to $\mathbf{K_B}$.
$\mathbf{P_{FB}}$ is the number of packets received from $\mathbf{K_B}$.

These data would be utilized by the monitoring nodes to incentive or punish the nodes in the neighborhood. Conditions described below gives the activities of nodes while monitoring neighborhood.

- A node '$\mathbf{K_A}$' forwards packet for other nodes is to be encouraged by awarding incentive credit. The incentive will be proportional to the number of packets forwarded.

- A compromised node '$\mathbf{K_A}$' may drop packets from other nodes. Therefore, if a node is found to drop packets more than a threshold value, only then it may be suspected and punish. Where '$\mathbf{T_{DROP}}$' is a preset threshold ratio for maximum permissible packet drops as normal behavior of the nodes.

- A suspected node '$\mathbf{K_A}$' is identified as a black-hole when it drops 100% of the packets. A black-hole is to be detected and punished accordingly. The punishment is set such that thei-rate value of a black-hole node falls below '$\mathbf{T_{i\text{-}rate}}$'.

- This is a case which is somewhat reverse in logic to the first rule. If a node is found to generate packets at an abnormal rate and more than a pre-set threshold value '$\mathbf{T_{GEN}}$', only then it would be suspected as a malicious node and punished as a suspected packet generating node is proportional to the ratio of packets generated spuriously.

- A compromised node '$\mathbf{K_A}$' may manipulate its own neighbor set and increase the value stored in the '$\mathbf{P_{TB}}$' field make false claim of incentives. The fact can be verified by looking up the neighborhood set '$\mathbf{K_{SB}}$' of node '$\mathbf{K_A}$'. A suspected node that makes false claim of packet forwarding may be doing so for long time. However, if it is detected as a black-hole, the i-rate degrades sharply. The mechanism thus has an inbuilt protection both against false alarms and serious malfunctioning caused by the disturbance.

VI. IMPLEMENTATION AND RESULT ANALYSIS

The proposed work is simulated using GLOMOSIM with the following metrics and evaluates the efficiency and effectiveness of protocols. The proposed method was simulated considering the following parameters as shown in Table 1.

TABLE 1: Simulation Parameters

Parameter	Value
Simulation area	2000 X 2000
Number of nodes	100
MAC layer	802.11
Transport layer	UDP and TCP
Traffic generator	CBR
Mobility model	Random way point
Node placement	Random
Routing protocol	AODV
Simulation time	500s

To evaluate the performance of data security the following parameters are analyzed:

- *Average throughput:* Measured as the ratio of data packets delivered to the destination to data packets originated by the source. This presents the routing efficiency of the protocol.
- *End-to-end delay:* Measured as the time interval from the moment that the source node sends a first message until the moment that the destination node in the network receives the last message. It also includes all possible delays caused by queuing at the interface, retransmission delays, propagation and transfer times.
- *Control overhead:* Measured as the number of control packets transmitted by all the nodes during the entire simulation.
- *Routing overhead:*Routing Overhead is the number of routing packets transmitted for every data packet sent.

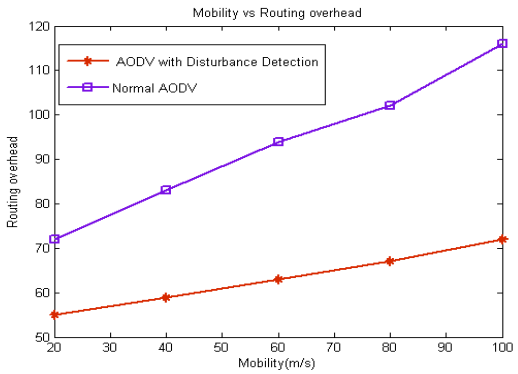

Figure 5: Mobility vsRouting overhead

Fig. 5 shows the evaluation of routing overhead with respect to mobility of nodes. We have analyzed the routing overhead with normal AODV and DDA AODV routing protocols. From the graph we observedthat as the mobility of the node increases, the routing overhead in DDA AODV is less compared to the normal AODV and also routing overhead increases gradually as the mobility increases in both the cases.

Fig. 6 shows the graph between number of packets transmitted vsthroughput. We analyze that the throughput almost remains constant in the case of DDA AODV when compared to normal AODV protocol.

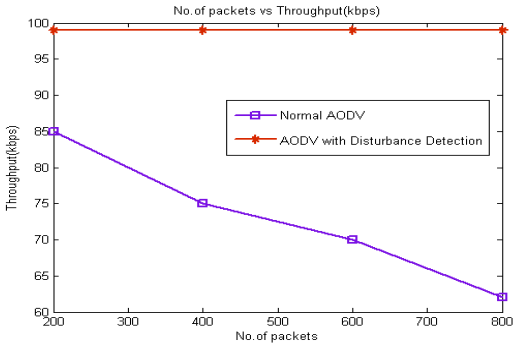

Figure 6: No. of packets vs Throughput

Fig. 7 shows the assessment of control overhead with respect to the network traffic in the case of higher mobility. From the graph it is observed that as the overall traffic in the network increases the control overhead increases by a route discovery process and mainly due to the number of route requests flooded in the network. This is mainly due to the frequent route failures, which in turn increases the number of route discovery process.

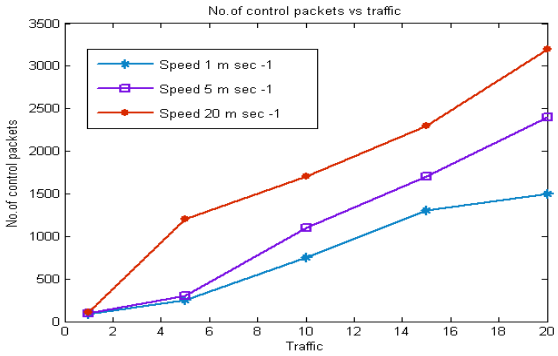

Figure 7: No. of control packets vs Traffic

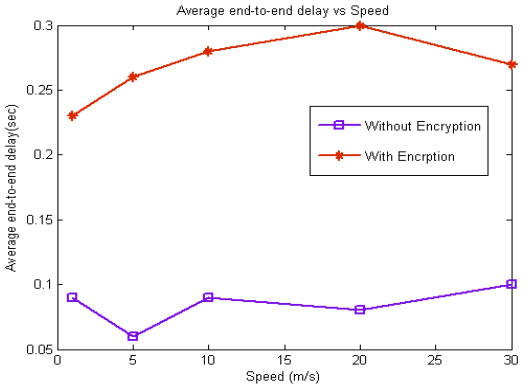

Figure 8: Average End-to-End delay vs Speed

Due to encryption a finite delay is introduced in the transmission of packets since the entire file is encrypted in the transmitted side and decrypted in the receiver side. The observed delay is found to be greater than compared to delay without encryption scheme. Initially delay decreases at lower mobility values, which may be attributed to the case when nodes come together. The delay of the data packets that wait for route discovery increases where as delay for all other data packets are unaffected. Therefore the increase in the end-to-end delay is fairly constant is shown in the Fig. 8.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have discussed a novel method for the data security cum authentication in mobile ad hoc network using the combination of symmetric and asymmetric algorithms. Also Disturbance Detection System is introduced to minimize/eliminate the malicious nodes. The proposed methodology was investigated on the performance of AODV with CBR traffic. We analyzed the protocol performance with both data security as well as with Disturbance Detection Algorithm and proved that the performance of the network is increased. As a future work, the strength of the proposed cryptographic algorithm should be analyzed by implementing Brute Force analysis.

REFERENCES

[1] Subir Kumar Sharkar, T.G.Basavaraju, C.Puttamadappa, "Ad hoc mobile wireless networks, Principles, protocols and applications", Auerbach PublicationsBoston, MA, USA©2007.

[2] H Yang, H Y.Luo, F Ye, S W.Lu and L Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, 2004, PP.38-47.

[3] DiaaSalama, HatemAbdual Kader and MohiyHadhoud, "Studying the effects of Most Common Encryption Algorithms", International Arab Journal of e-Technology, Vol.2, No.1, January 2011.

[4] A.L.Jeeva, Dr.V.Palanisamy, K.Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption algorithms", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol.2, Issue 3, May-June 2012, PP.3033-3037.

[5] S.A.Razak, S.M.Furnell, P.J.Brooke, "Attacks against Mobile Ad hoc Networks Routing Protocols", In Proceedings of 5th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PGNET 2004, 2004.

[6] ShashiMehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms For Data Communication", IJCST Vol.2, Issue 2, June 2011.

[7] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish", Journal of Global Research in Computer Science, Vol.3, No.8, August 2012.

[8] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha, "Throughput Analysis of Various Encryption Algorithms", IJCST, Vol.2, Issue 3, September 2011.

[9] ChhayaNayak, "Performance of Various Algorithms Used in Cryptography", IJMIE, Vol.2, Issue 7.

[10] Gulshan Kumar, MritunjayRai and Gang-Soo Lee, "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement", International Journal of Security and Its Applications, Vol.6, No.1, January 2012.

[11] Gurjeet Singh, "Security Threats and Maintenance in Mobile ad hoc networks", IJECT, Vol.2, Issue 3, September 2011.

[12] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad hoc Networks - (A Survey)", The 17 th White House Papers Graduate Research In Informatics at Sussex, (2004), pp.1-23.

[13] Er.Deepinder Singh Wadhwa, Er.Tripatjot Singh Panag, "Performance Comparison of Single and Multipath Routing Protocols in Ad hoc Networks", Int. J. Comp. Tech. Appl., (IJCTA), Vol2, Sept-Oct 2011, PP.1486-1496.

[14] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A Counter Measure to Black hole Attack on AODV Based Mobile Ad hoc Networks", International Journal of Computer & Communication Technology(IJCCT), Vol.2, Issue 6, 2011.

[15] AmandeepKaur, "Trust Formalization In MANET Within Multichannel", International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN 2250-2459, Vol.2, Issue 6, June 2012.

[16] Adnan Nadeem and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communication Surveys & Tutorials, accepted for publication, 2013.

[17] Yao Yu, Lincong Zhang, "A Secure Clustering Algorithm in Mobile Ad hoc Networks", IPCSIT, Vol.29, 2012.

[18] AmandeepMakkar, Bharat Bhushan, Shelja and Sunil Taneja, "Behavioral Study OF MANET Routing Protocols", International Journal of Innovation, Management and Technology, Vol.2, No.3, June 2011.

[19] M. Madhurya, Dr. B. Ananda Krishna, "A Novel Cryptographic Algorithm for Data Security in MANETs", International Journal of Engineering Research and Technology (IJERT), PP.26-30.

[20] W. Stallings, "Cryptography and network security 4th Edition", prentice hall, 2005, PP.58-309.

Author's Biography

Ms.M.Madhurya graduated from Nova College of Engineering and Technology for Women, Vijayawada,in Electronics and Communication Engineering in the year 2011. Currently she is pursuing her Master degree in Digital Electronics and Communication Systems at Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt. AP.

Dr.Ananda Krishna B. graduated from Madras University in Electronics and Communication Engineering in the year 1999. He obtained his Master degree in Digital Electronics & Advanced Communication from Manipal Institute of Technology, Manipal and PhD in the area of Improving Quality of service through Secured Routing in Ad Hoc Networks at Jawaharlal Nehru Technological University, Hyderabad. Presently he is working as a Professor in the department of ECE at Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt. AP.

Mrs.T.Subhashini graduated from VR Siddhartha Engineering College, Vijayawada in the year 2005. She obtained her Master degree in Digital Electronics & CommunicationSystems from Gudlavalleru Engineering College, Gudlavalleru and her area of interest is Wireless Communication and Network Security. Presently she is working as an Assistant Professor in the department of ECE at Gudlavalleru Engineering College, Gudlavalleru, Krishna Dt. AP.

How to cite this paper: M.Madhurya, B.Ananda Krishna, T.Subhashini,"Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks", IJCNIS, vol.6, no.2, pp.30-37, 2014. DOI: 10.5815/ijcnis.2014.02.05

