ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/101372, December 2016* ISSN (Online) : 0974-5645

A Robust and Secure Lightweight Authentication for the Limited Resource Wireless Ad-hoc Network

Preet Kamal Sharma* and Dinesh Kumar

Department of Computer Application, Guru Kashi University, Talwandi Sabo, Bathinda – 151302, Punjab, India;
preetkamal20@gmail.com, kdinesh.gku@gmail.com

Abstract

Objectives: The proposed security model is specifically designed to increase the level of the security by implementing the node integrity verification and data encryption service over the wireless ad-hoc networks. **Methods/Statistical Analysis:** The proposed security and authentication model has been defined using the 8 bytes to 16 bytes length based variable key length authentication scheme, which is difficult to predict and cryptanalysis attacks, as there is no uniform mechanism to perform the cryptanalysis attack over the authentication data during the exchange or propagation in the wireless ad-hoc networks. **Findings:** In this paper, we have proposed the public cryptosystem based encryption for light and secure authentication scheme, which utilizes the RSA encryption as the public cryptosystems. The proposed security and authentication model has been deeply analyzed to protect against the variety of attacks using the primary parameter of authentication delay and data loss. This model has been analyzed over the three primary attacks for the resource jamming, which includes the Distributed Denial of Service (DDoS), selective jamming, and black hole attacks for the data dropping and jamming attacks. The proposed authentication and security model for wireless ad-hoc routing has been analyzed for its performance on the basis of the specific performance parameters. The robust and flexible performance of security and authentication based proposed model has been deeply observed from the versatile results obtained from the all paradigms of the simulation. **Application/Improvements:** The light weight and robust authentication based security mechanism has been proposed for the higher order suitability to serve the specific purpose of security against the attacks over the wireless networks.

Keywords: Ad-Hoc Network Security, Attack Prevention, Cryptanalysis Attacks, Jamming, Light Authentication

1. Introduction

Wireless ad-hoc networks are the networks, who can construct the topology automatically by deploying the primary connections as well as the cluster center or the network management nodes. The ad-hoc network is generated in such a way that it provides real time information and analysis of low level data in hostile environment[1]. The wireless nodes communicate with each other in the absence of physical network via radio signal. The wireless networks work as transmission media among several devices[2]. The wireless ad-hoc networks are considered as the self controller and self-governed devices, which are considered to be the equipped with the limited memory compositions and limited power microcontrollers Figure 1. The wireless ad-hoc nodes are designed with the limited backup sources as they carry the smaller batteries[3-4].

*Author for correspondence

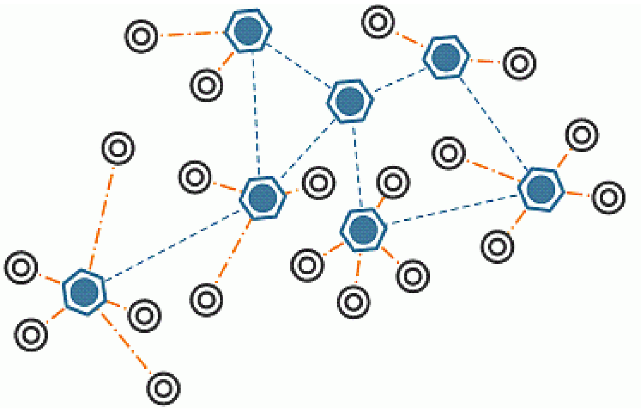

Figure 1. An example of wireless ad-hoc network (Wireless Network)[5].

The communication or information provided by wireless networks are expected to have data integrity, the data which is transfer by the sender is not temper or modified on the path from sender to receiver[5]. In the wireless network time synchronization is expected such that there is absence of delay in packets when it is transfer between two nodes[6-7]. Confidential information is anticipated in wireless network it denotes particular information must be prevented from entrusted third party[8]. The nodes of wireless ad-hoc network are deployed in adversarial environment so it is vulnerable to attacks. Wireless networks are endangered to security attack owing to broadcast nature of transmission medium Figure 2[9].

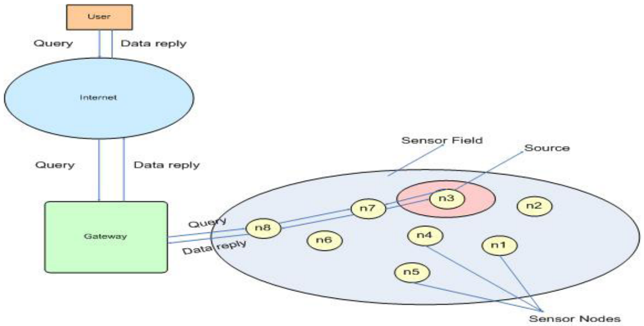

Figure 2. Internet Protocol (IP) based Wireless Adhoc Network[10].

The major application of the wireless ad-hoc networks includes the healthcare monitoring, telemedicine, environmental monitoring, wildlife monitoring and tracking, entertainment industry, home and office automation and security applications, variety of the data collection and surveillance based military applications, logistics and many other research and application specific areas.[10] One of the major examples of the ad-hoc network applications lied in the Kenyan Forest Wildlife Monitoring Project or Congo Forest Wildlife Monitoring projects for the tracking and analysis of the animal movement across the year with changing situations and seasons. [10-11] Also the ad-hoc networks have been utilized to study the micro-climatic conditions in the specific regions, such as Lahaul and Spiti, Himachal Pradesh and Leh, Jammu and Kashmir of India.[12] In the case of the military related applications, the ad-hoc network deployment has been discovered across the border areas for the surveillance and activity monitoring, battlefield updates and monitoring, [13] where the information is either propagated from or towards the soldiers or the vehicles carrying the target wireless objects Figure 3[14].

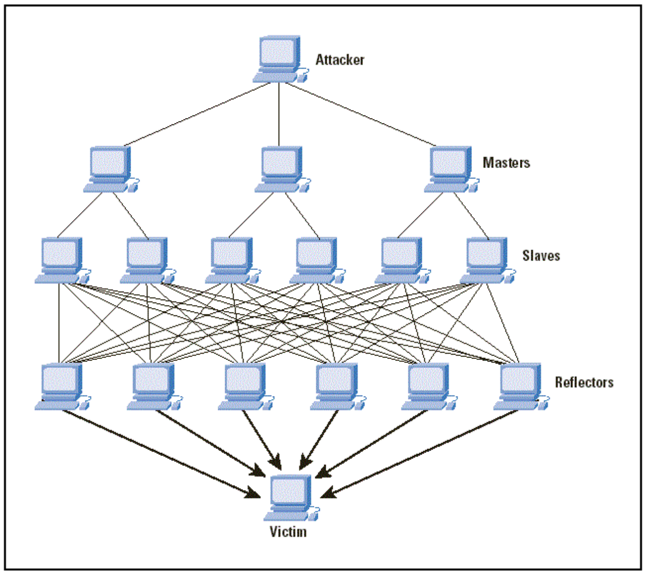

Figure 3. An example of hierarchical DDoS attack[15].

The technological advancements in wireless communication and microelectronics have resulted in a growing interest in the wireless ad-hoc networks[16]. The wireless ad-hoc networks involve the distributed topology based live monitoring of the real-life events and situations[17]. The use of the ad-hoc networks has widened during the past decades and the incursion of ad-hoc networks in the variety of the real-life applications[18]. These applications of the ad-hoc networks has made this very important for implementation of the higher order of security infrastructure. The deployment of these networks in military applications and the limited power and memory, make the security and network architectural design of the proposed model is complex and challenging[19]. In this paper, the primary issues related to security have been adaptively designed for the directed diffusion and security levels of the proposed security model for the ad-hoc networks[20]. A look-in to possible attacks and counter measures is provided. The paper is concluded with a brief analysis on the possible countermeasures to prevent such attacks[21].

Abraham bestowed the new data packet during the propagation during the transmission, and protects the data transmissions for the target packets traversing or transiting through the target nodes or paths[22]. During this theme every packet traversing constant path carries constant symbol. Path symbol fits in every single packet therefore the victim will straight off filter traffic when receiving only 1 attack packet[23]. In[24], the authors have proposed an efficient routing protocol energy, which is hierarchical and based cluster. In this protocol, the base station selects Cluster Heads (CH). The selection procedure is carried out in two stages. In the first stage, all candidates to become nodes CH are listed on the basis of parameters such as the relative distance of the wireless nodes from the base transceiver station and the remaining energy levels. The cluster head generates two schedules for the cluster members know sleep and TDMA transmission function. The performance of the proposed protocol is compared with that of LEACH by simulation experiments. It is noted that the proposed protocol outperforms LEACH in all circumstances considered in the simulation. In[25], the authors have worked on the ad-hoc network consists of hundreds of thousands of wireless nodes collect various data, such as sound, temperature, location, etc. They have been applied in many fields such as health, the surveillance system, the military, and so on. It is mainly difficult to replace the sensor nodes that have limited battery capacity[26]. Energy efficiency is a key challenge in maintaining the network. In this paper, the author proposes a method of selection of the head effectively clustered using K-means algorithm to optimize the energy efficiency of wireless sensor networks[27]. It is depends on the concept of finding the cluster head reducing the sum of the Euclidean distances between the nodes of the head and member[28].

2. Experimental Design

The proposed model is based upon the dual layer encryption authentication for the protection against the data dropping attacks over the wireless ad-hoc networks. The proposed authentication model is semi-centralized and semi-supervised model, which works in the dual stage authentication between the wireless node nodes. The proposed method is using random key table of two columns, where for each key $K_{Q,}$ a key K_A is available. K_Q is a question key, which carries an answer key $K_{A.}$ All of the keys in the table (question/answer keys) are generated using a random function which is non-track-able and non-trace-able. The new scheme will add least overhead because it will not generate key at every time. It will generate the key table on the starting phase and will share the pre-generated key table across the neighboring nodes. Each and every node will shares the authentication key only during the first packet exchange of a packet stream between two wireless node nodes. This scheme will be capable of handling both DoS and DDoS attacks.

2.1 RSA Encryption

The RSA encryption model is based upon the public-private key based encryption. The RSA is the first age public-key cryptosystem and has been used in variety of applications. The RSA algorithm utilizes the public key based upon two prime numbers with large values and one auxiliary value. The RSA algorithm design has been described below:

2.1.1 RSA Key Generation

The RSA key pairs requires to be generated in the pair of the private and public keys, which are shared between the both end nodes or people in order to share the information securely in the encrypted form between the both ends. It is very important to keep the encryption key pairs knowledge securely. The owner of the information requires keeping the private key very secretly in order to protect the complete communication. The smarted key generation plays the vital role in the authentication model, which utilizes the following algorithm:

Algorithm 1: Key generation

- Firstly, generate the larger prime number ranging between 512 digits to 1024 digits for the security enhancement.
- Then, the modulus is calculated over the input value or number (denoted p and q).

- Afterwards, the quotient value is computed over the index factor n, (n).
- Construct the public key from the generated numbers, which lies between the range [3, (n))], which obtained by dividing the (n) with the divisor of first rotation.
- Then construct the private key, which is generated from the (n).

2.1.2 RSA Encryption

When the sender to send the message to somebody, the sender encrypts the message by using the public-key provided by the receiver. The cipher data is forwarded to the receiver's end.

2.1.3 RSA Decryption

The receiver node is intended to reveal the data by using the decryption paradigm by utilizing the private key in the key pairs.

Algorithm 2: RSA Enc/Dec Process

- The RSA algorithm is used to transform the plaintext information into the cipher or the input data. The primary inputs of the public cryptosystem function lies with the message or string m or key k, which can be described as following:
  - F(m,k)=mkmodn**(9)**
- The two cases of encryption and decryption can be defined as the following:
  - Encryption key or Public key denoted with PbK, decryption key or private key denoted with PvK.
  - Encryption key or private key denoted PvK and decryption key or public key PbK
- The step 2a and step 2b interprets the mirrored cases for the public cryptosystem under the RSA mechanism
- The mirrored cases are the utilized on the different operations as per defined in the following formation:
  - F(m,e) equals memodn which is denoted with c, where input message (plaintext) is denoted with symbol m. e defines the public key and c denotes the output or cipher.
- The decryption can be defined as the following:

F(c,d)=cdmodn=m.

The proposed key model has been designed as the point-to-point centrally managed key scheme. The proposed model works in the server-client model, where the sender wireless node plays the role of server and the receiver wireless node connects as the client in the communication model. The Peer to peer authentication scheme has been proposed in this paper, which is entirely based upon the hybrid mechanism considered the semi-centralized mechanism. The proposed model has been specifically designed with the robust and lightweight authentication scheme by using the combination of the symmetric and asymmetric cryptography based dual-cryptography model. The following model explains the proposed authentication (Peer-to-Peer, Semi-centralized) model working in detail:

Algorithm 3: Key Scheme Algorithm Sequence for Function Calling

- The network topology is constructed after the neighbor formation
- The cluster manager node is defined in the topological nodes
- When a node requires to send the connection setup request towards the another node
  - The route is requested
  - If the route is reachable
    - The sender is requested to send the confirmation towards the receiver node
    - The connection setup request is forwarded
- If the node accepts the connection setup request and returns the positive acknowledgement
  - Further, the sender node initiates the node integrity check
  - If the node integrity check returns true
    - The route is accepted
  - Otherwise
    - The route is rejected
    - Communication request is refused

3. Result Analysis

The dual layer based encryption has been proposed for the new authentication and security model in this paper. The proposed security and integrity model is designed by aiming at the requirement of the robust security for the network links to protect against the data dropping attacks in the wireless ad-hoc networks. The lightweight authentication scheme has been proposed in this simulation, which has been evaluated for its performance against the existing model for the vital and clear performance parameters.

The data loss or packet loss is the parameter indicates the data lost during the communication between the two given points within the given simulation. The data loss occurs due the attack over the Ad-hoc networks. In the following Figure 4, the performance assessment and evaluation is completed over the results obtained from both of the models (Existing and proposed) along with the graphical representations. The results of the proposed security and integrity model have been obtained with the quite lower value at nearly 5000 bytes as the data loss, where the existing model shows the whopping 100 thousand bytes of the data loss during the transmissions.

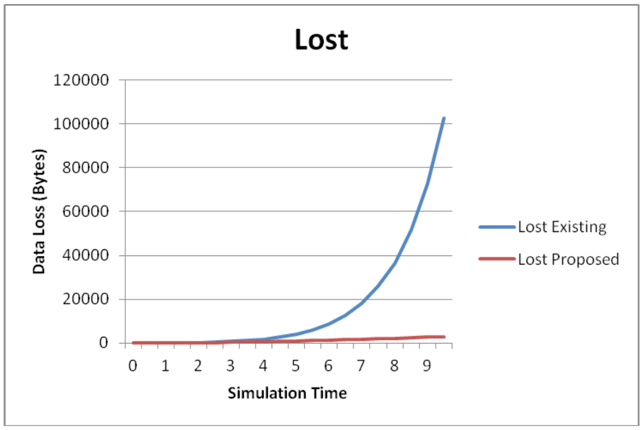

Figure 4. Data loss for blackhole simulation.

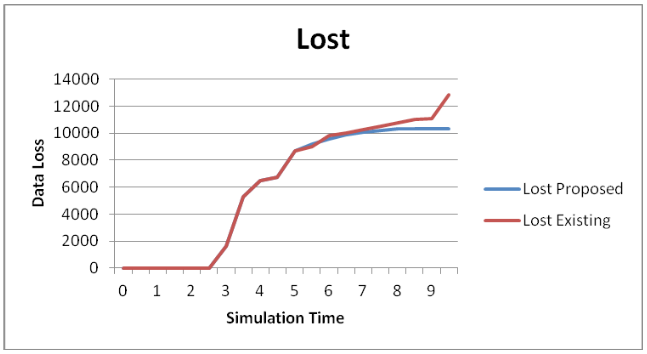

Figure 5. Data loss for DDoS simulation.

In the case of black hole attack, the data is lost over the specific node, which is attacked and programmed as the black hole node in the Ad-hoc network is shown in Figure 5. The DDoS attack is mitigated by dropping the overflow data and starts receiving the needed data. The low amounts of lost data during the DDoS show the effectiveness of the proposed model in mitigating the overflow of data on the ingress port. As the DDoS, the selective jamming attack is also based upon the packet flooding towards the target node, but from the single node, which differentiates the selective jamming and DDoS attack. The proposed model has been also been effective against the selective jamming attack, which is indicated via the Figure 6 and 7 which shows the less volume of attack data drop by the proposed model in comparison with existing model Table 1.

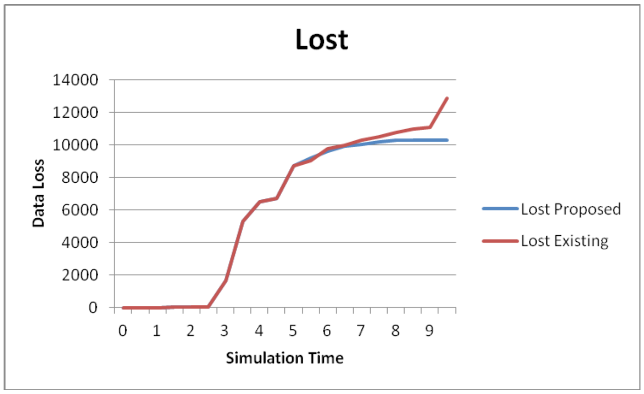

Figure 6. Data Loss for multi-node Selection Jamming

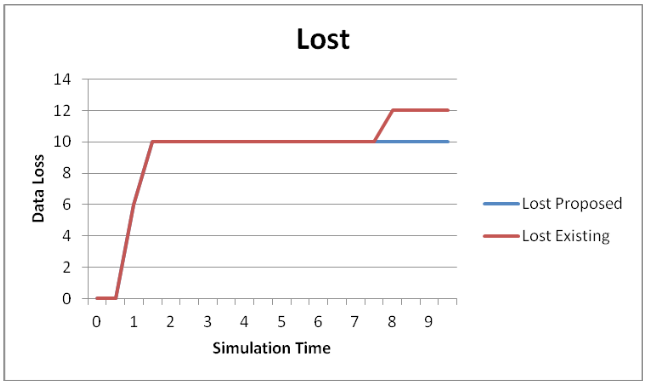

Figure 7. Data loss for selective jamming simulation.

Table 1. Table of Data Loss of all three simulations

	Lost		
Simulation Time	Selective Jamming	DDoS	Blackhole
0	0	0	1
0.5	0	0	2
1	6	0	3
1.5	10	8	33
2	10	8	101
2.5	10	8	205
3	10	1652	323

3.5	10	5290	457
4	10	6514	601
4.5	10	6744	765
5	10	8712	931
5.5	10	9032	1115
6	10	9792	1303
6.5	10	10002	1507
7	10	10290	1721
7.5	10	10502	1945
8	12	10752	2193
8.5	12	10992	2453
9	12	11110	2735
9.5	12	12868	3033

The transmission delay includes the time taken by the packet in the transmission over the network media, waiting time in the queue and other such causes of delay. Only the packets with the successful delivery status are considered for the calculation of the transmission delay in the simulation scenario. When the nodes transmit the data in the inter-cluster formation, the congestion is caused over the communications links after the link overloading with the higher volumes of data. Such heavier volumes in result, increases the transmission delay from the given WIRELESS NETWORK scenario.

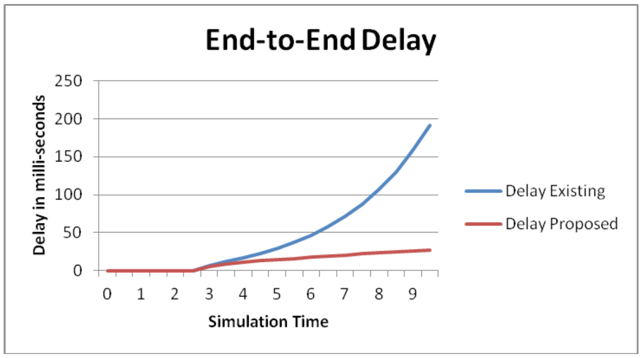

Figure 8. End-to-end delay for black hole simulation.

In the Figure 8 the model proposed on the basis of double encryption based authentication model in this research has been found offering the lower transmission than the existing model, which is being used for the comparative analysis in this section. The proposed model has been recorded with the reading of nearly 25 milli-seconds of the transmission delay against the 200 milli-seconds in the existing model, when tested over the simulation with the black hole attack. The following Figure 9 has also justified the robust performance of the proposed model in the terms of end to end delay in comparison with the existing model.

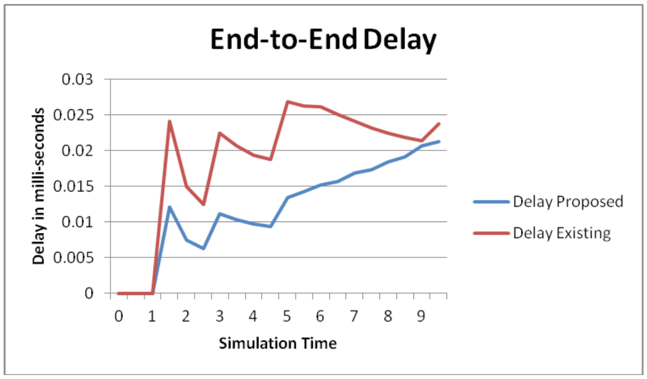

Figure 9. End-to-end delay for DDoS simulation.

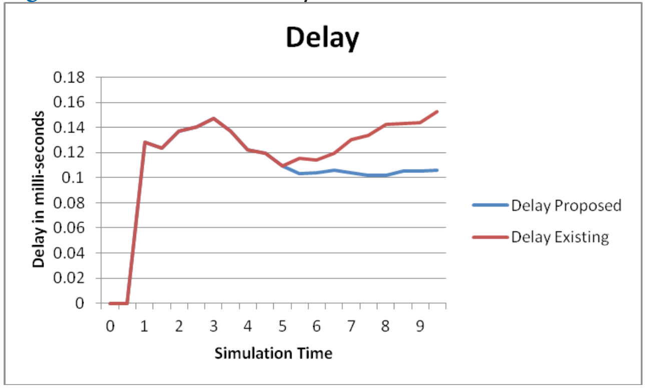

Figure 10. End-to-End Delay for Selective Jamming simulation.

In the Figure 10, the pattern has not been changed and remained similar to black hole and DDoS attack simulations in mitigating the attack against the existing model. The proposed model has been found almost 15-20% efficient in mitigating the attack data in comparison with the existing model Table 2.

Table 2. Table of delay for all three simulations

	Delay		
	Selective Jamming	DDoS	Blackhole
0	0	0	0
0.5	0	0	0
1	0.128350553	0	0
1.5	0.123333792	0.024154935	0
2	0.137124753	0.015015629	0
2.5	0.140766833	0.012499953	0
3	0.147160525	0.022465183	5.900935921

3.5	0.136825386	0.020637625	8.978129928
4	0.122388893	0.019395773	10.95364764
4.5	0.119551491	0.018761099	12.92916535
5	0.109279391	0.026859106	14.53231232
5.5	0.115592975	0.026329848	16.13545928
6	0.114396644	0.026190759	17.61529905
6.5	0.119753815	0.025095553	19.09513882
7	0.130653421	0.024089519	20.64024952
7.5	0.133700004	0.023241714	22.04251332
8	0.142302214	0.022511302	23.44477712
8.5	0.143415217	0.021903832	24.78204866
9	0.143890371	0.021456591	26.11932019
9.5	0.152861013	0.023815516	27.44808308

4. Conclusion

The dynamic key generation policy has empowered the authentication process with the high number of keys in the secure space using the cryptography mechanism. The key management policy includes the RSA encryption, which is public-key cryptosystem, and based upon the public and private keys, where the network data is secured with encryption utilizing the Public key (PbK) and decryption process utilizes the Private Key (PrK) or vice-versa. The RSA cryptosystem is named after the inventors Ron Rinvest, Adi Shamir and Leonard Adleman. The RSA has been empowered with the new key generation policy which makes it securer than its previous version. The proposed mode authentication has been designed for the higher level of security to avoid the attacker nodes from joining the network. The active traffic and pattern analysis capability of the network Intrusion Detection System (IDS) empowers the proposed model to analyze the anomalies in the traffic to avoid the attack on the given segment of the ad-hoc networks. The proposed model has been consistently found improved for the mitigation of the attacks such as selective jamming, black hole and DDoS attacks in accordance with the existing model designed to tackle the similar problems.

5. References

1. Agrawal R, Tripathi R, Tiwari S. Performance evaluation and comparison of AODV and DSR under adversarial environment. Proceedings of the International Conference on Computational Intelligence and Communication Systems; India. 2011.
2. Anuj K, Gupta G, Sadawarti H. Performance analysis of AODV, DSR and TORA Routing Protocol. IACSIT. 2010; 2(2):226-31.
3. Bala A, Bansal M, Singh J. Performance analysis of MANET under black hole attack. ICNC; India. 2009. p. 141-5.
4. Chandramouli R, Iorga M, Chokhani S. Cryptographic key management issues and challenges in cloud services computer security division information technology laboratory. NIST; 2013. p. 1-36.
5. Chen L, Tang H, Wang J. Analysis of VANET security based on routing protocol information. 4th International Conference on Intelligent Control and Information Processing (ICICIP); Beijing, China. 2013. p. 134-8.
6. Damgard I, Thomas P, Jakobsen J, Nielsen JB, Jakob I, Pagter P. Secure key management in the cloud cryptography and coding. Lecture Notes in Computer Science. 2013; 8306:270-89.
7. Ehsan H, Aslam Khan F. Malicious AODV: Implementation and analysis of routing attacks in MANETs. Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications; 2012.
8. Fuad A, Ghaleb M, FauziIsnin ARI. Security and privacy enhancement in VANETs using mobility pattern. IEEE 5th International Conference on Ubiquitous and Future Networks (ICUFN); Malaysia. 2013.
9. Zayandehroodi H, Hamzehbabaei, Eslami M. Optimization of energy consumption in cooperative wireless network using quadratic programming. Indian Journal of Science and Technology. 2015 Dec; 8(35):1-7.
10. Hung CC, Chan H, Wu EHK. Mobility pattern aware routing for heterogeneous vehicular networks. IEEE WCNC; 2008.
11. Govindarajan J, Devi GA, Kousalya G. Analysis of TCP-unfairness from MAC layer perspective in wireless ad-hoc networks. Indian Journal of Science and Technology. 2015 Aug; 8(18):1-8.
12. Jacob J. Performance analysis and enhancement of routing protocol in manetvol. IJMER. 2012; 2(2):323-8.
13. Joao A, Dias D, Joao N, Isento I, Vasco NGJ, Soares S, Farahmand F, Joel JPC. Rodrigues test bed-based performance evaluation of routing protocols for vehicular delay-tolerant networks. IEEE. USA. 2011.
14. Khabazian M, Ali MKM. A performance modeling of Vehicular Ad Hoc Networks (VANETs). IEEE Wireless Communications and Networking Conference (WCNC); 2007.
15. Khiavi1 MV, Jamali S, Gudakahriz SJ. Performance comparison of AODV, DSDV, DSR and TORA routing protocols in MANETs. International Research Journal of Applied and Basic Sciences. 2012; 3(7):1429-36.

16. Kuppusamy P, Thirunavukkarasu K. A study and comparison of OLSR, AODV and TORA routing protocols in ad hoc networks. India. 2011. p. 143-7.
17. Lamyaa MT, Harb M, Tantawy T, Elsoudani M. Performance of mobile ad hoc networks under attack. International Conference on Computer Applications Technology (ICCAT); 2013. p. 1201-6.
18. Morshed MDM, Islam MDR. CBSRP: Cluster based secure routing protocol. IACC. 2013; 3(2):571-6.
19. Muhammad A, Javed J, Jamil Y, Khan K. A geo-casting technique in an IEEE 802.11p based Vehicular Ad hoc Network for Road Traffic Management. Australasian Telecommunication Networks and Applications Conference (ATNAC); Australia. 2010.
20. Ramya P, Gopalakrishnan V. An efficient timer based minimum path D-equivalence CDS construction for wireless adhoc networks. Indian Journal of Science and Technology. 2015 Apr; 8(S7):1-9.
21. Park GY, Kim H, Jeong, Youn HY. A novel cluster head selection method based on K-means algorithm for energy efficient wireless sensor network. 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA); South Korea. 2013. p. 910-5.
22. Seuwou P, Patel D, Protheroe D, Ubakanma G. Effective Security as an ill-defined problem in Vehicular Ad hoc Networks (VANETs). IET and ITS Conference on Road Transport Information and Control (RTIC 2012); UK. 2012.
23. Sheng L, Shao J, Ding J. A novel energy-efficient approach to DSR based routing protocol for ad hoc network. Proceedings of the International Conference on Electrical and Control Engineering; 2010.
24. Suganthi N, Sumathy V. Energy efficient key management scheme for wireless adhoc network. Int J Comput Commun. 2014; 9(1):71-8.
25. Sumra IS, Hasbullah H, MohsanIftikhar JA, Ahmad I, Mohammed Y, Aalsalem A. Trust levels in Peer-to-Peer (P2P) vehicular network. IEEE 11th International Conference on ITS Telecommunications (ITST); Malaysia. 2011.
26. Tiloca M, Guglielmo DD, Dini G, Anastasi G. SAD-SJ: A self-adaptive decentralized solution against selective jamming attack in wireless adhoc network. ETFA. 2013; 18(1):1-8.
27. Tuteja A. Comparative performance analysis of DSDV, AODV and DSR routing protocols in MANET using NS2. ICACE. 2010; 330-3.
28. Yadav S, Lakhani K. A cluster based technique for securing routing protocol AODV against black-hole attack in MANET. International Journal of Distributed and Parallel Systems. 2013; 4(2):17.