International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 685-693 June 2018-Dec 2018 www.csjournals.com

An IDEA-HMAC Cryptography Based Secure AODV Routing Protocol for Routing Attack Prevention in MANET

[1]T.Kamaleshwar, [2]Dr.K.Venkatachalapathy
[1] Ph.D. Scholar, Department of Computer Science & Engineering, Annamalai University, Chidambaram, India
[2] Professor & Head, Department of Computer & Information Science, Annamalai University, Chidambaram, India
[1]kamalesh4u2@gmail.com, [2]omsumeetha@rediffmail.com

Abstract: MANETs are a deal of portable nodes which are self-designing and related by remote connections naturally according to the characterized directing convention. These nodes speak with one another by trade of packets, which for those nodes not in remote range goes jump by bounce. Extraordinary attributes, for example, dynamic system topology, constrained data transmission, and restricted power, hubs running on battery steering in a MANET is an especially difficult errand contrasted with a customary system The major attacks in a wireless MANET are black-hole, worm-hole and man in the middle attacks. These attacks are related to network layer that spoil the entire network by falling-packets. The attacker attains such type of attacks where all of the similar kinds of nodes transmit data to another. The responsibility of the MANET is to protect network layer from various types of attacks. An advanced secured cryptographic model is essential to defend such type of malicious elements. In this work, Secure IDEA-HMAC based AODV routing protocol for preventing routing attacks in MANET. The detection of the three major attacks can be addressed in MANET with accuracy by using such type of technique. IDEA is the best to implement as an advanced cryptographic model with the better security level within the limited energy constraint. To enhance authentication, a symmetric key IDEA encryption is used, an hash message authentication code (HMAC) uses a cryptographic hash function coupled with a secret key for secure message transmission and communication among the mobile nodes in networks. In addition, this algorithm used to add scalability to the AODV routing protocol to prevent against routing attacks in MANET. Thus this proposed IDEA algorithm also ensures authentication, encryption and integrity of the message which are transmitted via mobile adhoc network.

Keywords: Intrusion detection, IDEA, AES, AODV, HMAC

Introduction

The MANET (Mobile Adhoc Network) refers to the multi-hop packet of wireless network made out of ambulant nodes which can convey and move at a same time, by unusable type of wired framework [1].

MANET is a well-organized and adaptable framework which is formed without any incorporated association. A MANET is abbreviation of Mobile Adhoc network that location can be changed and designed on the fly. These are portable to use with the remote alliances by the interface of different systems. The occasion of MANET working set is to get a standard internet routing protocol utility that's appropriate for any mobile routing application inside both stable and active topologies which expands to a vital range because of node motion and different elements [2].The methodologies are consciously lightweight in nature and suitable for various hardware in portable situations to address the scenarios where MANETs are conveyed to the boundary of an IP groundwork. Hybrid mesh work is a framework that must be upheld with MANET's determinations and management factors. Utilizing full-fledged components on the test WG will create two standard track routing protocol specifications: Reactive MANET Protocol (RMP) and Proactive MANET Protocol (PMP) [4]. Some attacks are obstacle for data transmission in MANET. Blackhole attack, Denial-of-service attack(DOS), Greyhole attack, Wormhole attack, Jelly fish attack and man in the middle attack are major among them. In this paper IDEA cryptography technique is employed for data security which detects the blackhole , worm-hole attacks and man-in-the-middle attacks. IDEA Cryptography is a symmetric by nature. It has better resistance command over differential cryptanalysis technique which makes utilization of different group of operations to raise its quality against usual recognizable attacks. IDEA comprises of 128 bit of key that provides a better security. No direct or algebraic attack has been efficient to break key within a stipulated time. The process applies to all keys can divide IDEA in 6 rounds.

In IDEA Cryptography both encryption and decryption are similar. Different operations are performed to achieve the higher level security. Operations in IDEA cryptography are as follows:

- Bitwise exclusive OR operation..
- Addition modulo of 216.
- Multiplication modulo of 216+1.

This will be helpful in data transmission by availing better security to thwart the defined attacks.

The proposed Secure IDEA-HMAC based AODV routing protocol for preventing routing attacks in MANET . It uses private or shared key cryptography techniques for securing the message and routing path during the communication. Course disclosure in AODV utilizes Route Request RREQ and Route Reply RREP, Containing two sorts of data fields named as Mutable and Non Mutable Hope count is the only mutable field as intermediate nodes increment the hope count field while forwarding the RREQ and the rest of fields such as IP address, Sequence Number are non mutable fields as they remain unchanged. the proposed AODV uses two mechanism to secure routing in MANETs.

i) for authenticating the non mutable field of routing message M, use HMAC(KSD , M)
ii) for authenticating the mutable field, which means hope number details, the one way $HMAC$ key chain is used

Thus the proposed IDEA – HMAC scheme is used to detect intrusions under various attacks such as black hole, wormhole, routing loop, selfishness, and sleep deprivation in Mobile Adhoc Networks environment.

Existing System

MANET will communicate with different wireless nodes with each other without having the proper infrastructure. Where the security of such system is a noteworthy concern.. The symmetric cipher algorithm allows us to store the data in a compressed encryption form which results in a small size database. Also it performs faster encryption/ decryption. In order to perform the encryption and decryption of data, so we are using the symmetric cipher algorithm. This will also serve confidentiality. This method is applied on AODV protocol for securing the data. And results are compared with the normal AODV and this secured. First we find the route to the node to which we wish to communicate. For this we use the concept the broadcast the control message using AODV routing protocol. i.e. With the routing protocol AODV we search for the required node. When we found the node the receiving node sends route reply message. If any malicious node attempts to establish the connection then with the help of IP address we come to know about it and we can divert the traffic towards receiver through another route. We can vary the keys sizes in AES algorithm. In order to improvise the security of this kind of network, the method of AODV routing protocol through the use of symmetric encryption algorithm like AES. This will secures the data and also it prevents the confidentiality.

Problem Statement

To accomplish secure correspondence in MANET a few necessities must be fulfilled

(a) A security affiliation must exist between system individuals; these security affiliations guarantee validation and non renouncement for confided in hubs.
(b) Sensitive data must be traded secretly between the hubs in the system.
(c) Integrity of the data traded inside the system must be kept up with the goal that debased messages are identified and blocked.
(d) AES uses too simple algebraic structure.
(e) Every block is always encrypted in the same way.
(f) Hard to implement with software.
(g) AES in counter mode is complex to implement in software taking both performance and security into considerations.

Proposed System

The specially appointed systems are defenseless against assaults because of disseminated nature and absence of framework. It give review and observing capacities that offer the neighborhood security to a hub and help to see the particular trust level of different hubs. In the current work AES encryption calculation is utilized for secure steering in MANET. AES encryption has exceptionally basic logarithmic structure and furthermore every square is encoded in a similar way , it has complex execution in programming regarding both security and execution . The obligation of the MANET is to shield arrange layer from different kinds of assaults. A progressed anchored cryptographic model is basic to shield such sort of noxious components.

In this work, an IDEA-HMAC calculation for AODV directing convention is proposed for secure message transmission, steering in MANET. This calculation is proposed to recognize any malevolent hub exercises. The IDEA is utilized for encryption, it is one of the protected and most generally utilized square figures and the cryptographic quality of IDEA depends on a blend of three contradictory gathering tasks – XOR, expansion and particular duplication. To improve validation, for the IDEA encryption, a hash message confirmation code (HMAC) utilizes a cryptographic hash work combined with a mystery key for secure message transmission and correspondence among the versatile hubs in systems. Furthermore, this calculation used to add versatility to the AODV steering convention to avert against directing assaults in MANET. This proposed calculation additionally guarantees verification, encryption and respectability of the message which are transmitted by means of versatile adhoc organize.

TECHNIQUES USED

1) IDEA Algorithm

International Data Encryption calculation (IDEA) is a square figure calculation planned by Xuejia Lai and James L. Massey of ETH-Zürich and was first portrayed in 1991.The unique calculation experienced couple of alterations lastly named as International Data Encryption Algorithm (IDEA). The made reference to calculation takes a shot at 64-bit plain content and figure content square (at one time). For encryption, the 64-bit plain content is partitioned into four 16 bits sub-squares. In our talk, we indicate these four squares as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits). Every one of these squares experiences 8 ROUNDS and one OUTPUT TRANSFORMATION stage. In every one of these eight adjusts, a few (number juggling and legitimate) tasks are performed. All through the eight ROUNDS, similar arrangements of tasks are rehashed.

In the last stage, i.e., the OUTPUT TRANSFORMATION stage, we perform just number juggling activities. Toward the start of the encryption procedure, the 64 bit plain content is separated in four equivalent size squares and prepared for ROUND1 input. The yield of ROUND1 is the contribution of ROUND2. Additionally, the yield of ROUND2 is the contribution of ROUND3, et cetera. At last, the yield of ROUND8 is the contribution for OUTPUT TRANSFORMATION, whose yield is the resultant 64 bit figure content (expected as C1 (16bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)). As the IDEA is a symmetric key calculation, it utilizes a similar key for encryption and for decoding. The unscrambling procedure is the equivalent as the encryption procedure with the exception of that the sub keys are inferred utilizing an alternate calculation [6]. The extent of the figure key is 128bits. In the whole encryption process we utilize add up to 52 keys (ROUND1 to ROUND8 and OUTPUT TRANSFORMATION stage); created from a 128 piece figure key. In each round (ROUND1 to ROUND8) we utilize six sub keys. Each sub-key comprises of 16 bits. What's more, the OUTPUT TRANSFORMATION utilizes 4 sub-keys.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 685-693 June 2018-Dec 2018 www.csjournals.com

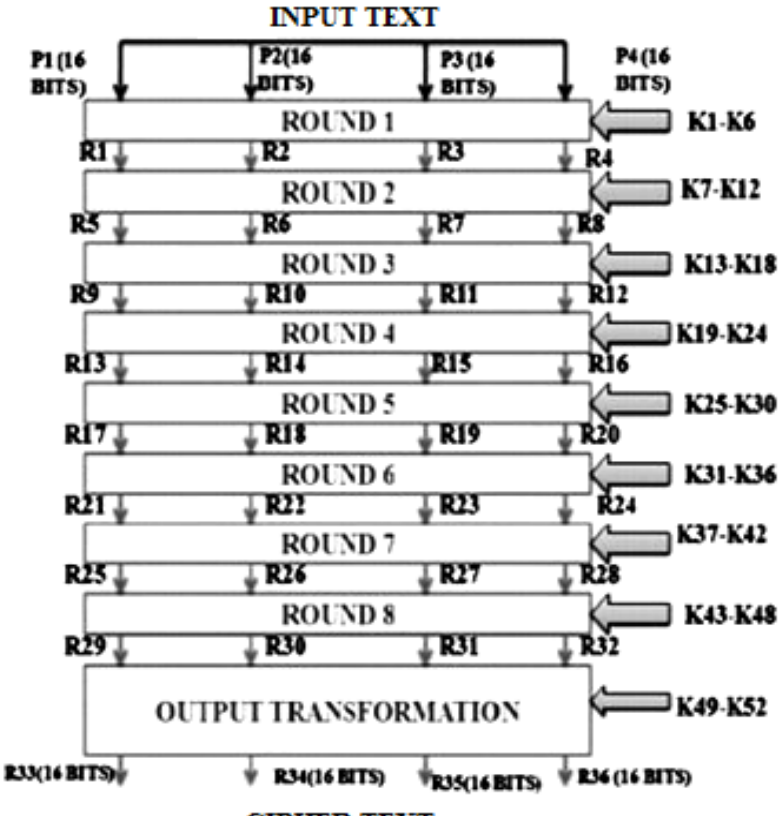

Fig 1 : IDEA Encryption Algorithm

i) IDEA Algorithm – For Encryption

To encrypt the message the IDEA Algorithm is used
1. Multiplying X1 and the first subkey Z1
2. Sum X2 and therefore the second subkey Z2
3. Sum X3 and therefore the third subkey Z3
4. Multiplying X4 and therefore the fourth subkey Z4
5. Bit Shift XOR the results of steps one and three.
6. Bit Shift XOR the results of steps two and four.
7. Multiplying the result of step 5 and the fifth subkey Z5'.
8. Suming the results of steps six and seven.
10. Multiplying the results of step eight and therefore the sixth subkey Z6'
11. Suming Up the results of steps seven and nine.
12. Bitshift XOR operation for the results of steps one and nine.
13. Bitshift XOR operation for the results of steps three and nine.
14. Bitshift XOR operation for the results of steps two and ten.
15. Bitshift XOR operation the results of steps four and ten.

ii) Decryption Process

- The procedure method used for secret writing of the cipher text is basically an equivalent as that used for encoding
- The solely distinction is that every of the fifty two 16-bit key sub-blocks used for secret writing is that the inverse of the key sub-block used throughout encoding.
- The sub blocks should be employed in reverse order than of the encoding spherical.

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 685-693 June 2018-Dec 2018 www.csjournals.com

2) HMAC Authentication

To enhance check for the message (HMAC) uses a cryptographic hash work joined with a mystery key. HMAC takes a variable number of contentions by basically connecting them and register the message confirmation code It is used to incorporate twofold encryption for secure message transmission and correspondence among the hubs in a systems. A hashed message affirmation code (HMAC) is a message verification code that makes use of a cryptographic key nearby a hash work. The genuine calculation behind a hashed message confirmation code is convoluted, with hashing being performed twice. This helpers in restricting a couple of sorts of cryptographic examination. A hashed message check code is believed to be more secure than other relative message affirmation codes, as the data transmitted and enter used as a piece of the method are hashed freely. In particular, hash works that perform well in programming, and for which code is straightforwardly and by and large available. It use and handle keys fundamentally

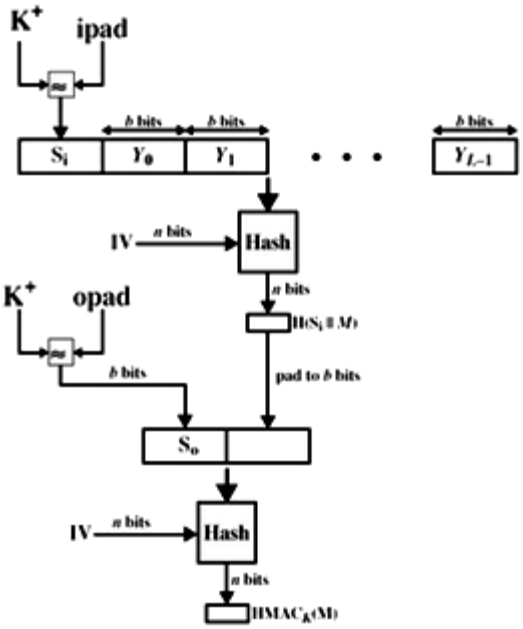

Fig 2 : HMAC Authentication

The security of mac add context of an put in hash work depends only on some ways on the cryptographical plan of the lined hash work. The keenness of HMAC is that its modelers have might demonstrate an accurate relationship between the concept of the inserted hash work and therefore the idea of HMAC. the protection of a mac work is for the foremost half passed on the degree that the probability of profitable manufacture with a given extent of your time spent by the beguiler and a given range of message-MAC sets created with a equal key. Basically, it's a bent to be displayed that, for a given level of effort (time, message-MAC sets), on messages created by real shoppers and seen by aggressors, the probability of a gain attack on HMAC is unclear to 1 of the running with ambushes on the bestowed hash work

1. Aggressors will inscribe a yield of the burden work even with associate degree Initial price (IV) that's isolated, puzzle, and cloud to attackers.

2. Aggressors realize impacts within the hash work once the IV is unpredictable and mystery.

In the principle assault, you'll see the pressure work as equivalent to the hash work related to a message together with a lone b-bit sq.. For this assault, the IV of the hash work is supplanted by a mystery, unpredictable estimation of n bits. A strike on this hash work needs either a beast constrain assault on the key, that could be a level of effort on the request of 2n, or a birthday assault, that is a unprecedented prevalence of the second assault.

In the second assault, aggressors ar looking down 2 messages, M and M', that create a comparative hash: H(M)=H(M'). this needs level of sweat of 2n/2 for a hash length of n. To assault MD5, assailants will decide any arrangement of messages and work on these disconnected on a submitted calculation workplace to seek out a crash. Since assailants understand the hash calculation and therefore the default IV, aggressors will deliver the hash code for every one in every of the messages that aggressors create. In any case, whereas assaulting HMAC, aggressors cannot produce message/code sets disconnected in lightweight of the method that assailants do not know K. Thusly, aggressors should watch a rendezvous of messages delivered by HMAC beneath a comparable key and play out the strike on these famed messages. For a hash code length of 128 bits, this needs 264 watched squares (273 bits) created employing a comparative key. On a 1-Gbps interface, you'd ought to watch a tireless stream of messages with no modification within the key for around 250,000 years to succeed. on these lines, if speed could be a worry, it's entirely ample to use MD5 instead of SHA-1 or RIPEMD-160 because the embedded hash work for HMAC.

i) HMAC Algorithm – For Authentication

1.Make the length of K equal to b.
2. XOR K with Ipad to produce S1.
3. Append M to S1.
4. Message-digest algorithm.
5. XOR K with opad to produce S2.
6. Append H to S2.
7. Message-digest algorithm.

HMAC Algorithm uses shared IDEA symmetric key to encrypt message digest.

Simulation Results

This work shows the simulation results generated after detecting black hole attack, wormhole attack and man in the middle attacks. To avoid the effect of these three attacks. This work makes use of IDEA- HMAC algorithm based secure AODV routing protocol for IDS detection technique. Thus the simulation is evaluated, it shows that sending node is sending the messages to receiving node properly. It shows that CBR packets are reaching from source node 0 to the destination node 1 as expected. With this secure cryptography based AODV routing protocol has nullified the effect of intrusion. In this way, this work have detected an intrusion in ad hoc network and avoided its effect in the network. As we have nullified the effect of black hole, wormhole and man in the middle attack in the network, the performance of the network is improved. The charts which are produced by actualizing our answer for interruption in intrusion system. It shows that the secure AODV routing protocol has improved the packet loss, delay, transmission data rate and throughput of the network. Thereby the routing overhead of the MANET has been reduced.

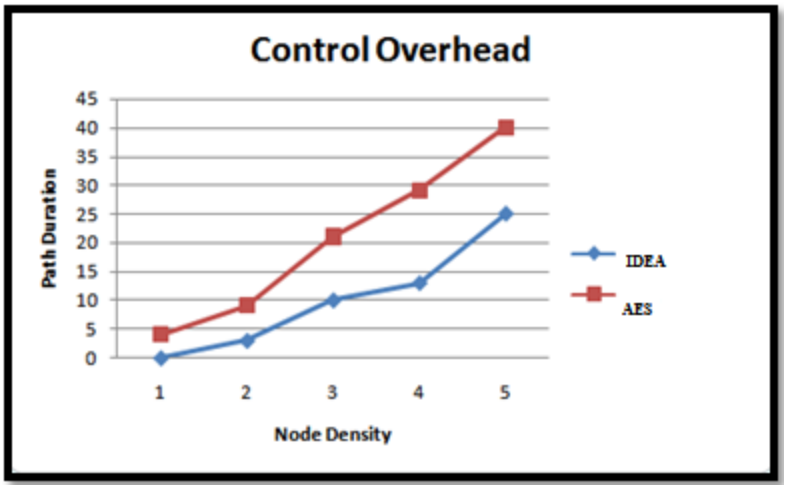

Fig 3 . Control Overhead

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 685-693 June 2018-Dec 2018 www.csjournals.com

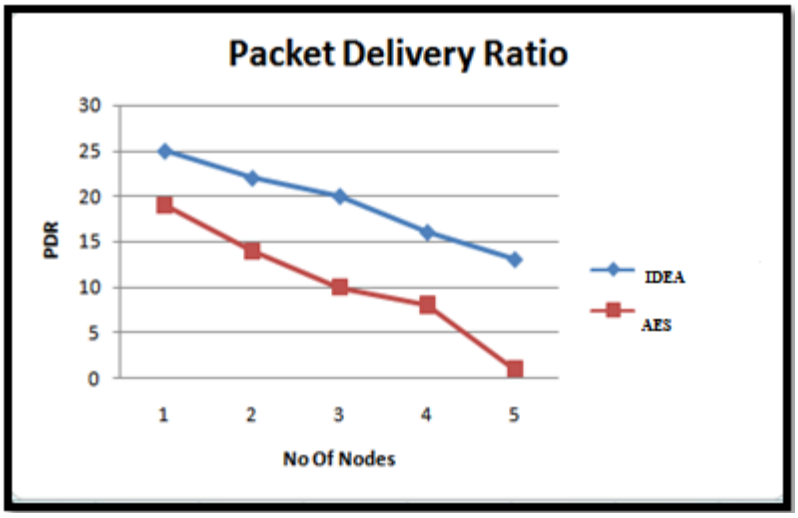

Fig 4. Packet Delivery Ratio

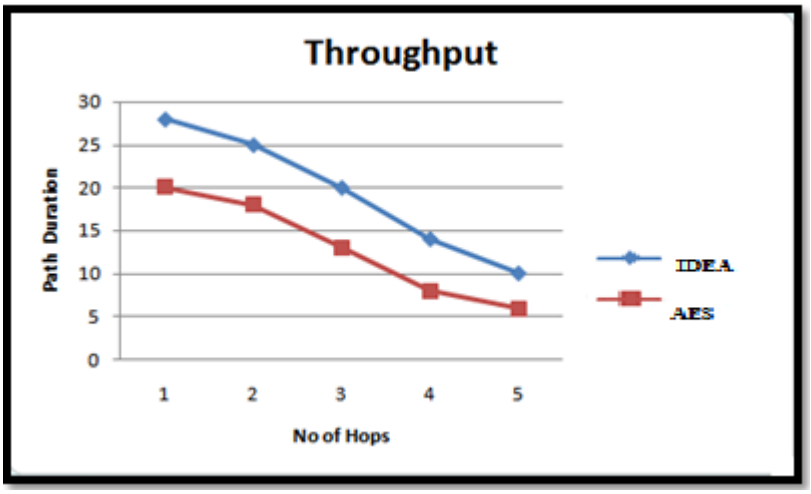

Fig 5 . Throughput

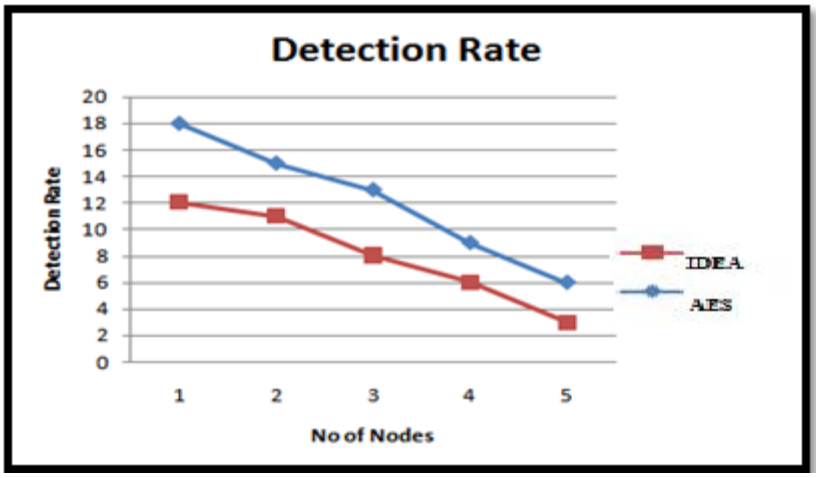

Fig 6 Detection Rate

Conclusion

Thus, in this paper secure routing is one of the issues in MANET. In the existing work , AES encryption algorithm is used for secure routing in MANET. AES algorithmic structure has some limitations , AES encryption has very simple algebraic structure and also every block is encrypted in the same manner , it has complex implementation in software in terms of both security and performance . The responsibility of the MANET is to protect network layer from various types of attacks. For providing better performance, AODV routing of MANETs uses IDEA- HMAC algorithm during the establishment of secure route between source node and destination node. In the proposed, secure AODV routing approach for pairs of node share a IDEA symmetric key and through this key, the message is encrypted and secure communication between intermediate node by signing and verifying the RREQ message during traveling from one node to other nodes. The simulation result concludes that secure cluster based AODV routing method minimizes the time delay and network control packet overhead involved in computation and verification of security fields during route discovery process. The results found that proposed algorithm for secure cluster based AODV routing perform much better than the normal AODV routing when number of malicious nodes present in the network because normal AODV does not have any security mechanism while proposed algorithm for secure based AODV routing protocol uses hashed message authentication code for providing authentication and integrity of the message.

References

[1] Huseyin Demirci, Ali Aydn Selcuk and Erkan Ture " A New Meet in the Middle Attack on IDEA Block Cipher , 2005.

[2] H. Elkamchouchi, Fatma Ahmed, " Enhanced Idea Algorithm For Strong Encryption Based On Efficient Strong Rotor Banks " , 2011.

[3] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, "Securing On-Demand Source Routing in MANETs ", IEEE Explore Digital library, 2010, pp:294-297.

[4] K.Sangeetha, "Secure Data Transmission in MANETS Using Eliptic Curve Cryptography", International Journal of Innovative Researchin Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014, pp:2557-2562.

[5] A article on "Next Generation Encryption" , Cisco security intelligence operations, April 2014

[6] Stephan Eichler, Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", München, Germany, IEEE *Xplore* Digital Library, 8-2006.

[7] Zahra Moradlu, Mohammad Ali Doostari, Mohammed Gharib, " Fully Distributed Self Certified Key Management for Large-Scale MANETs", 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing on Autonomic & Trusted Computing,pp:96-102.

[8] Tameem Eissa, Shukor Abdrazak, Md Asri Ngadi, " Enhancing MANET Security using Secret Public Keys "2009 International Conference on Future Networks , IEEE, pp:130-134.

[9] Soma Saha , Rituparna Chaki , Nabendu Chaki , " A New Reactive Secure Routing Protocol for Mobile Ad-Hoc Networks", IEEE computer society(2008), pp:103-108

[10] Thandu Naga Srinu Padma, Tandu Ramarao, Nischala Simhadri , "AODV Routing Protocol in MANET based on Cryptographic Authentication Method ",Vol 2, Issue10, IJCSET |October 2012,ISSN-2231-0711,pp:1459-1464.

[11] Luciano Bononi and Carlo Tacconi, "A Wireless Intrusion Detection System for Secure Clustering and Routing in Ad Hoc Networks",2006.

[12] 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.

[13] Chong Eik Loo And Mun Yong Ng ,"Intrusion Detection for Routing Attacks in Sensor Networks", *International Journal of Distributed Sensor Networks*, 2: 313–332, 2006.

[14] Shimbre, Nivedita, and Priya Deshpande. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm." *Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on* IEEE, 2015.

[15] Meera, K., P. Krishna Sankar, and K. Sriram Kumar. "Redundant file finder, remover in mobile environment through SHA-3 algorithm." *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*. IEEE, 2015

[16] Ajay Vikram Singh, Moushumi Chattopadhyaya, "Mitigation of DoS Attacks by Using Multiple Encryptions in MANET", 2015 4th IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 at AUUP, NOIDA, India, September 02-04, 2015.
[17] Kanmani, P., and S. Anusha. "A novel integrity scheme for secure cloud storage." *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*. IEEE, 2015.
[18] Lenka, Sudhansu Ranjan, and Biswaranjan Nayak. "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm." *International Journal of Computer Science Trends and Technology (IJCST)– Volume* 2 (2014).
[19] Fips pub 198, the keyed-hash message authentication code.
[20] W. stallings, cryptography and network security: Principles and practices, 3rd edition, prentice hall, 2003.
[21] Nist: Secure hash standard, fips 180-1, national institute of standards and technology, u.s. department of commerce (May 1994).
[22] et al., B.W.: A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security Springer, 17 (2006).
[23] Aziz, B., Nourdine, E., Mohamed, E.K.: A recent survey on key management schemes in manet. 3rd International Conference on ICTTA pp. 1-6 (April 2008).
[24] D.Djenouri, L.Khelladi, N.Badache: A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys and Tutorials Journal 7(4), 2-29 (December 2005).
[25] Deng, H., Li, W., Agrawal, D.P.: Routing security in wireless ad hoc networks. IEEE Communications Magazine 40(10), 70-75 (October 2002).
[26] Fall, K., Varadhan, K.: Ns-2, the ns manual (formally known as ns documentation) available at http: //www. isi.edu/nsnam/ns/doc.
[27] Hu, Y., Johnson, D.B., Perrig, A.: Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA). pp. 3-13 (June 2002).
[28] Hu, Y.C., Johnson, D.B., Perrig, A.: Ariadne: A secure on-demand routing protocol for ad hoc networks. Proc. 8th Ann. Intl Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press pp. 12-23 (September 2002).
[29] Hu, Y.C., Perrig, A.: A survey of secure wireless ad hoc routing. IEEE Security and Privacy 2(3), 28-39 (May-June 2004).
[30] Issariyakul, T., Hossain, E.: Introduction to network simulator ns2 (July 2008). Johnson, D.B., Maltz, D.A.: The dynamic source routing protocol in ad hoc wireless networks. In: Mobile Computing, Kluwer Academic Publishers. vol. 353, pp. 153-181 (1996).
[31] P.Albers, O. Camp, J. M. Parcher, B. Jouga, L. Me, R. Puttini. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. WIS 2002. 4th Int'l Conf. on Enterprise Information Systems, 2002.
[32] T.Clausen,P.Jaquet,A.Laouti,P.Minet,P.Muhlethaler,A.Quyyum,L.Viennot, Optimized Link State Routing Protocol , Internet Draft, draft-ietf-manetolsr-06.txt, work in progress, Sep 2001.
[33] C. E. Perkins, P. Bhagwat, Highly Dynamic Destination-Sequenced DistanceVector Routing (DSDV) for Mobile Computers , Proc. of the SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications, Aug. 1994.
[34] D. B. Johnson, D. A. Maltz, Y-C Hu, J. G. Jetcheva, The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR), Internet Draft, draft-ietf-manet-dsr07.txt, work in progress, Feb 2002.
[35] Joan Daemen, Ren6 Govaerts and Joos Vandewalle "Weak Keys for IDEA", Springer Advances in Crytology , 2002.
[36] S. Bhargava and D. P. Agrawal. Security Enhancements in MAODV protocol for Wireless Ad Hoc Networks. in Proc. of Vehicular Technology Conference, 2001.
[37] H. Deng, W. Li and D. P. Agrawal. Routing Security in Wireless Ad Hoc Networks.IEEE Communications, October 2002.
[38] P. Ning and K. Sun. How To Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols. in Proceedings of the 4th Annual IEEE Information Assurance Workshop, pages 60-67, West Point, June 2003.