International Journal of Engineering & Technology, 7 (4.28) (2018) 717 -722

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Secure Trust based Routing Protocol for Scheme Enhancing Quality of Service in Mobile AdHoc Networks

G. Sripriya, Dr. T. Santha

Abstract

-Security is an essential requirement for any kind of networking. Security for MANET is more complicated due to its free infrastructure, decentralization and limited resources. So many protocols are designed for the security of MANET. Key management scheme is one of the schemes used in MANET for its high security. In this paper, Threshold based public key management scheme is applied to the On-Demand Vector Routing Protocol for the better performance and high security. Simulation using Network Simulator-2 (NS-2) and under various network conditions shows that threshold based public key management with On-Demand Vector Routing Protocol can greatly improve security and performance in terms of packet delivery ratio, routing overhead and energy consumption.

Keywords

1.Introduction

AD-HOC Networks is a network connection used to share files without the use of a router or a wireless base station. It is one of the temporary network connection created for a particular task. Mutli-hop ad hoc network is used to share files with more than one computer. In Mutli-hop ad hoc network multiple nodes are utilized for data transmission. MANET, stands for Mobile AdHoc Network, a self-configuring infrastructure less network. MANET is used where the communication infrastructure is not existed previously.
An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol made for mobile ad hoc networks. Both unicast and multicast routing could be supported by this protocol. In AODV protocol only after the request of source nodes routes between nodes could be built. So an extra traffic was avoided in AODV.
Multicast Ad Hoc On-Demand Distance Vector (MAODV) is a routing protocol used for multicasting. MAODV is designed for the quick adoption of low network utilization, dynamic link conditions, low processing and memory overhead. Tree based protocol and mesh based protocol are the classification of Multicast routing protocols. Single path between a sender and a receiver in the tree based protocol whereas multiple paths between sender and receivers in a meshed route.
While sharing files from one device to other device its security is more important than any other factors. Security service involves authentication, confidentiality, integrity, access control and availability. Due to dynamic topologies and membership, vulnerable wireless link and roaming in dangerous environment security in MANET is the challenging task. For secured Ad-hoc network, it is necessary to provide security architecture.
In this paper, Trust threshold based public key management secure multicast ad-hoc on demand vector routing protocol was described. For maximizing performance and to reduce security vulnerability, Composite Trust-based Public Key Management (CTPKM) is used. Here to determine whether or not to trust another node, each node employs a trust threshold. Simulation results show that an optimal trust threshold gives better performance, best security when compare to the existing protocol. Risk involved in the security also be neglected by using this trust threshold based public key management method. In this approach, to meet both performance and security requirements, a soft security approach is involved.
The remainder of this paper is organized as follows. Section2contains the review of some related work. Section3 presents the trust threshold based public key management with on-demand vector routing Protocol and Section 4contains simulation results. Finally, Section 5 concludes this paper.

2.Related Works

Zapata and Asokan (2002) have proposed a new routing protocol SAODV (SecureAd Hoc On-Demand Vector) by applying some modifications in conventional AODV (Ad Hoc On-Demand Vector).Here key management scheme is used to solve the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Digital signature and hash chains are the two mechanisms used to secure the ADOV messages.
Yang and Sun (2017) have proposed a routing protocol DMAODV (Distensible Multicast Ad Hoc On-Demand) which is developed from MAODV. All nodes in the network were allowed to send multicast data packets along multicast tree and broadcast features were fully utilized here. This work justified that DMAODV protocol has less control overhead, higher scalability and better performance when compare to MAODV.
Loganathan and Purusothaman have introduced an energy efficient key management and authentication technique for multicasting in MANET (Mobile Ad hoc Networks).By this key management authentication technique fault-tolerance was enhanced and the tree was protected from impersonation attacks. An energy efficient topology aware key tree was constructed to reduce the re-keying load. This can be reduced by pre-processing the joining members during the interval of idle re-keying. Diffie-Hellman key pair and RSA secret public key pair is the techniques which involved in this key management. A trust authority establishes public key certificates for each group member by signing the public key with its secret key.
Gowdaand Hiremath(2013) have presented a review of security approaches in routing protocol in MANET(Mobile Adhoc Network).Here a number of routing protocols, security services and types of attacks were explained. This work discussed mainly about the two categories of routing protocols for MANETs. Proactive and Reactive are the two categories of routing protocols. Routing

protocols were chosen based on the amount of network traffic and number of flows.

Borkar et al (2017) have proposed trust based secure Optimal Route Selection and Enhancing QoS in Mobile Ad-Hoc Networks by applying AOMDV-SAPTV and DE-Algorithm. By using Secure Closest Spot Trust Certification protocol (SCSTC) and the optimal link path is derived from Dolphin Echolocation Algorithm (DEA),a net based multicasting routing scheme was introduced which is used to discover all possible secure path. By this proposed technique the quality of routing could be enhanced and trusted path was found by optimization algorithm.

Younis et al (2012) have made a TAM (Tiered Authentication of Multicast) Protocol for Ad-Hoc Networks. For large scale dense ad-hoc networks TAM was introduced. The advantages of the time asymmetry and the secret information asymmetry paradigms were combined by the TAM. To reduce overhead and ensure scalability, a network clustering was exploited here. Delivery delay can be reduced using this protocol.

Hu et al (2005) have proposed Ariadne protocol for Ad Hoc Networks. Ariadne a new secure on-demand ad hoc network routing protocol. Tampering of compromised nodes with uncompromised routes and many types of Denial-of-Service attacks could be prevented by this protocol.

Curtmola and Nita-Rotaru (2017) have proposed BSMR (Byzantine-Resilient Secure Multicast Routing) in Multi-hop Wireless Networks. For the purpose of multicast services, Multi-hop wireless networks have relied on node cooperation. Vulnerabilities of on-demand multicast routing protocols for multi-hop wireless networks and the challenges encountered in designing mechanisms to defend against them were discussed. To withstand insider attacks from colluding adversaries BSMR was designed. BSMR is a software-based solution so hardware need not be used. The identified attacks were mitigated by BSMR.

Vedhavarshini and Anandhave(2017) have proposed efficient data packet transmission in MANET by using enhanced hybrid cryptographic technique. To avoid packet data loss in network, various Intrusion Detection System (IDS) were analyzed in this paper. Here Hybrid key cryptography scheme is used in MANET to avoid routing overhead by destroying malicious node's route.

Zamani and Zubair (2014) have proposed key management scheme in Mobile Ad Hoc networks and also secure and efficient key management scheme in MANETs. Main purpose of these two papers was providing secure methods for handling cryptographic keying algorithm.

Du and Xiong (2011) have proposed a dynamic key management scheme for MANETs. Jabbar et al (2017) has proposed power-efficient routing schemes for MANETs. Various power-efficient routing schemes in MANETs have reviewed, and here protocols are classified into six categories. Dangi and Tiwari (2016) have introduced a secure hybrid communication approach for disaster recovery system in MANETS. Singhi and Pippal(2018) have analyzed key management schemes in MANET. A novel secure Identity-based key management protocol was proposed. Ayman (2014) has proposed a new hierarchical group key management based on clustering scheme for mobile ad hoc networks. Wu et al (2009) has introduced an efficient group key management scheme for mobile ad hoc networks. Cho et al (2013) have described composite trust-based public key management in mobile ad hoc networks.

Hamouid and Adi (2010) have introduced Secure and robust threshold key management scheme for ad hoc networks. Gomathi and Parvathavarthini (2010) have developed an efficient cluster based key management scheme for MANET with authentication. Capkun et al (2003) has introduced a fully self-organized public-key management for mobile ad hoc networks. This allows users to generate their public-private key pairs. It does not require any trusted authority. Rhee et al (2004) has introduced architecture for key management in hierarchical mobile ad-hoc networks. Pužar et al (2005) has introduced Skimpy, a simple and efficient key management protocols used for MANETs in emergency and rescue operations.

3.Trust Threshold Based Public Key Management with On-Demand Vector Routing Protocol

3.1. Public Key Management

In Mobile Ad Hoc Networks (MANETs), public key management has been researched for many years. But designing a fully distributed public key management protocol under resource constrained MANET environments is great challenging task because of the unique characteristics of MANETs. Decentralized trusted entities, resource constraints, and high security vulnerabilities are the challenges in the key management. To eliminate security vulnerabilities, A fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust, instead of using hard security approaches as in traditional security techniques. Our work aims to maximize performance by relaxing security requirements based on the perceived trust.

3.1.1. Threshold Public Key Cryptography

Threshold cryptography based on sharing of secrets by generating a private key. In this threshold cryptography, the private CA key is distributed over a set of server nodes through a (k,n) secret sharing scheme. The private CA key is shared between n nodes in such a way that at least k nodes must cooperate in order to sign the certificates. However, a central trusted CA exists to select servers as the coordinators for key management, resulting in a single point of failure. In addition, the inherent weakness of the secret sharing scheme is the substantial delay when the set of trustworthy server nodes cannot be found to generate the private CA key. Besides, when the CA is compromised, the whole system is compromised.

3.1.2. Certificate-based Public Key Management

Certificate-based public key management approaches require public keys to be distributed where the receiving party should be able to authenticate the received key based on the certificate of the public keys. To deal with key management operations including key generation, distribution and revocation trusted CA is required. For MANETs without trusted CAs, certificate-based approaches should operate in a self-organized way.

3.1.3. ID-based Public Key Cryptography

ID-based Public Key Cryptography (ID-PKC) which generates a public key based on the ID of the node (e.g., IP or email address) and its corresponding private key generated by a trusted CA. Identity-based encryption is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Compared with typical public-key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. An added advantage is that a message recipient doesn't need advance preparation or specialized software to read the communication.

3.1.4. Hybrid Public Key Management

In cryptography, a hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations and are thus generally much more inefficient than comparable symmetric-key cryptosystems. In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive.

3.2. Attack Model

3.2.1. Packet Dropping:

A node may drop a packet received due to the nature of selfishness (e.g., to save energy) or maliciousness (e.g., to interrupt service availability). This is detected by overhearing to see if a packet sent to a neighbor for forwarding is actually being forwarded. It is not possible to tell if packet dropping is a problem of competence or integrity. Given that there are many attack behaviors that can be detected by our protocol design to attribute to integrity, to avoid double-count we simply attribute packet dropping to competence. If a node drops packets and the behavior is observed by a neighbor, this neighbor will decrease the misbehaving node's direct competence trust. Furthermore, this neighbor when acting as a recommender will propagate a negative recommendation to other nodes as indirect evidence against the misbehaving node.

3.2.2. Denial-of- service (dos):

A malicious node can generate unnecessary traffic to interrupt service provision in the system. We considered the DoS attack within the key management framework. Specifically, a malicious node can keep requesting public keys of other nodes even if it already has their valid public keys. Since only trustworthy nodes based on the trust threshold criterion are able to issue, distribute, and obtain key pairs, this DoS attack can consume network resources to increase delay of system operations, and reduce service availability. This attack is counter measured by using a trust threshold for intermediate nodes to ignore public key requests generated from a node whose trust level is below the threshold, thus effectively throttling DoS attacks.

3.3. Trust Model

3.3.1. Dimensions of Trust

Three trust components are considered to capture the unique aspects of trust in a MANET with communication, information and social networking:

• **Competence (C)** refers to an entity's capability to serve requests in terms of a node's cooperativeness and availability. Availability may be affected by network conditions such as link failure, energy depletion, and voluntary or involuntary disconnection (i.e., leaving the network). This is measured by the ratio of the number of positive experiences to the total experiences in packet forwarding.

• **Integrity (I)** is the honesty of an entity in terms of attack behaviors. This is measured by the number of positive experiences over the total experiences related to protocol compliance.

• **Social contact (SC)** is defined based on a node's inherent sociability derived from the trust profile available a priori as well as dynamic social behavior measured by the number of nodes that a node encounters during a trust update interval T u over the total number of nodes in the network. If an entity has high SC, it is more likely to disseminate information quickly to the network, compared to the ones with low SC. An entity's mobility pattern will affect this trust component.

3.4. Composite trust-based public key management

It is apparent that an effective key management frame-work for ad hoc networks must include a secure TTP but still encourage participation from as many nodes as possible. To address both of these principles, a novel paradigm for ad hoc key management is introduced that is called Composite Key Management, which uses a virtual CA and certificate chaining simultaneously in a single ad hoc network.

Each mobile entity is able to communicate with other entities using public/private key pairs obtained through CTPKM. In CTPKM, each node generates its own public/private key pairs periodically. But the key pair should be certified by a trusted third party which generates the certificate of the public key. Since CTPKM does not assume the existence of a trusted third party, each node needs to find the most trustworthy third party node among its 1-hop neighbors, called Neighborhood Trustworthy Certifier (NTC) which can certify the self-issued private/public keys.

In this trust metric used, the false detection can be reduced. The false can be detected by requiring the unanimous agreement of all intermediate nodes about the correctness of the recommendation delivered. The trust component X at time t is obtained by

$$T_{i,j}^{ID-X}(t) = \begin{cases} \frac{\sum_{kcR_j} T_{k,j}^{x}(t)}{|R_j|} \text{ if } |R_j| > 0 \\ \gamma T_{i,j}^{X}(t-\Delta t) otherwise \end{cases}$$

When nodes *i* and *j* encounter as 1-hop neighbors (i.e., *HD* (*i, j*) = *1*) during the time period *(t −_t)*, node *i*can collect direct evidence based on its own observations or experiences$P_{i,j}^{D-X}(t)$. When nodes *i* and *j* are distant with more than 1 hop distances, node *i* relies on its past experience to assess the direct trust of node *j*.

3.5. Secure multicast routing protocol

3.5.1. Secure MAODV Overview

This Secure MAODV(S-MAODV) protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial path. Here an authentication framework is used to remove outside adversaries and also to make sure that only authorized nodes perform certain operations. S-MAODV mitigates attacks that try to prevent a node from establishing a route to the multicast tree both in route request and route reply.

3.5.2. Trust Key Computing

New parameter weight value named TLv can be used to choose the best path. Trust value TLv is calculated by using following equation:

TLv = T(RREQ)* Qr + T(RREP)*Qp + T(MACT)*Qm + T(GRPH) * Qg+T(DATA)*Qd

Here function T is the weight value of category. These values are dynamically updated based on the successful delivery of a packet or receiving an error message. Upon receiving the route replies, best path will be chosen by the source depending on the serial number and average trust level value of the entire path which can be calculated as

TSTv=TLv/Hop Count

Hop count is the total number of intermediate devices such as routers through which a given piece of data must pass between the source and destination, instead of flowing directly over a single wire.

3.5.3. Secure Node Authentication

The authentication is designed to prevent the untrusted node to take part in the multicast tree. Here node sends RREQ/RREP only if the node from which RREQ/RREP is received must be a trust node. EveryNode maintains a neighbor list and marked it as not credible and unset enable flag in multicast routing table if neighbor's calculated trust value is less than the threshold NEIGH_UNSECURE.

3.5.4. Route Discovery

This route discovery allows a node which wants to join a multicast group or has a message to send to the multicast group to find a route to the multicast tree. Only group trusted nodes can initiate route requests to prevent outsiders from interfering. A field named TLv introduced to carry the information of degree on route's reliability.

3.5.5. Random Packet Forwarding

A node needing a route floods the network with ROUTE REQUEST packets in an attempt to find a route to the destination in MAODV. Each node typically forwards only one ROUTE REQUEST originating from any Route Discovery to reduce the overhead of this flood. In the traditional packet forwarding scheme all on-demand routing protocols only forward the request that arrives first from each route discovery. This traditional route request is replaced with the Random Packet forwarding scheme. This ensures that the paths with less delay are only likely to be selected than other paths. The idea is to gather n RREQ packets and choose any one arbitrarily for forwarding procedure. In case if the desired number of RREQ packets is not received then a node will wait for a source for particular period of time, before it randomly choosing and forwarding a packet. In each route discovery, before sending data packets, the source will collect a number of RREQ packets to do a selection. This selection is based on the highest serial number and the highest trust value.

4. Proposed Secure Multicast Ad-Hoc on-Demand Distance Vector Psmaodv

In this proposed protocol the combination of above Composite trust-based public key management and the S-MAODV concept were included for the better performance and security. CTPKM technique is included for trust threshold Key by considering three different trust dimensions, namely, competence, integrity, and social contact then a new parameter weight value named TLv can be used to choose the best path.

4.1. Simulation and Result Analysis

To evaluate the effectiveness of PSMAODV with the adversary model NS-2 simulator system is utilized. The simulation is made by varying the number of malicious nodes. Packet Delivery Ratio (PDR), Routing Overhead (RO), Energy Consumption (EC) are considered to assess the performance of our proposed scheme. The performance of PSMAODV is compared to SMAODV and AODV with the adversary model to prove that PSMAODV can achieve better routing decisions. The harmless nodes were distributed randomly throughout the network which employs the AODV, SMAODV and PSMAODV protocols. Randomly positioned nodes perform various packet forwarding misbehaviors according to the adversary model. Table 1 summarizes the simulation parameters.

Table 1: Simulation parameters. constant bit rate (cbr); user datagram protocol (udp).

Parameter	Value
Simulator	NS 2.34
Routing Protocol	AODV, Adversary Model, TSQRS
Scenario Size	1000 _ 1000 m2
Number of Nodes	50
Misbehaving Nodes	0–40%
Simulation Time	240 s
Traffic Type	CBR/UDP
Number of Connections	15
Pause Time	5 s
Mobility	4–20 m/s

4.2. Evaluation Considering the Percentage of Malicious Nodes

In this simulation, by only varying the percentage of malicious nodes between 0 and 40%, the performance of AODV (Ad-hoc On Demand Distance Vector), SMAODV (Secure Multicast Ad-hoc On Demand Distance Vector) and PSMAODV (Proposed Secure Multicast Ad-hoc On Demand Distance Vector) is evaluated.

Packet Delivery Ratio (PDR): Figure 1 explains that the number of packet drops can be expanded by increasing the percentage of malicious nodes, in which under the adversary model, PDR of AODV decreased to about 40% whereas SMAODV provides 45%. PSMAODV achieves 65%, it shows an improvement in PDR when compared to AODV and SMAODV. The number of dropped packets is reduced with the help of trust mechanism used in PSMAODV.

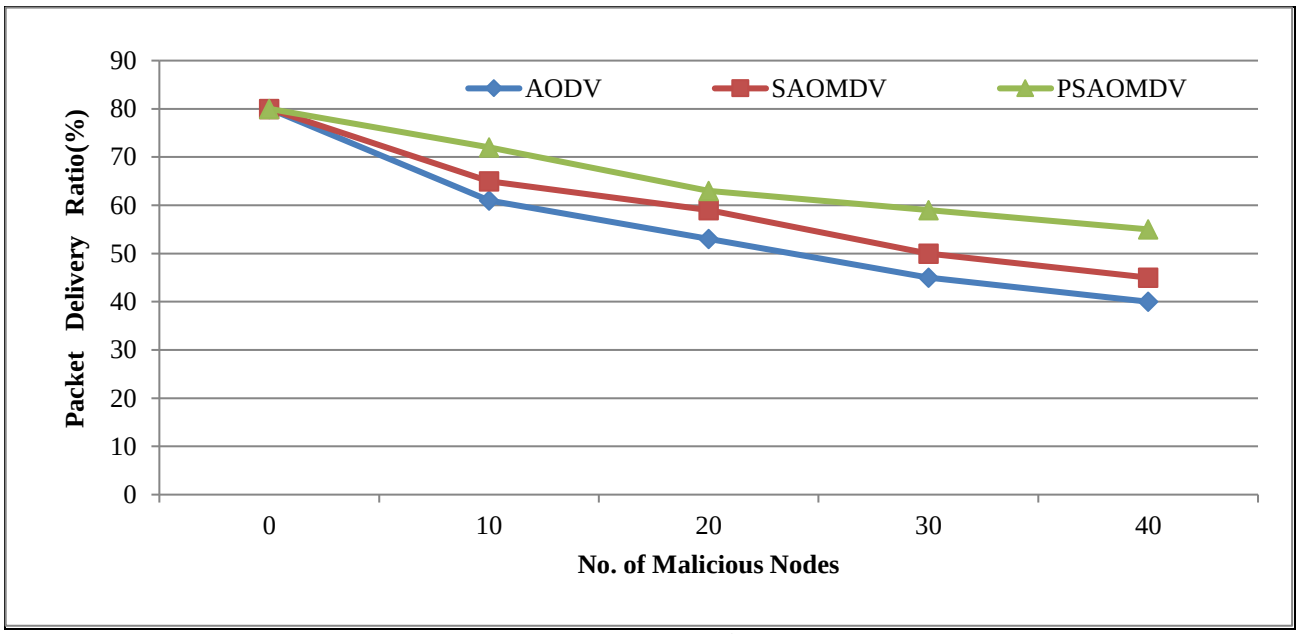

Figure 1: PDR against Percentage of Malicious Nodes

Routing Overhead (RO): Figure 2 explains that the RO of AODV in the range 5 to 10 while SMAODV again enhances RO to the range of 5 to 7 to under the adversary model. PSMAODV achieves improvement by ranging 5 to 6.4. Increase in number of malicious nodes can cause more damage. But in PSMAODV, it selects only the nodes having secure good link quality so that the number of route failures is decreased.

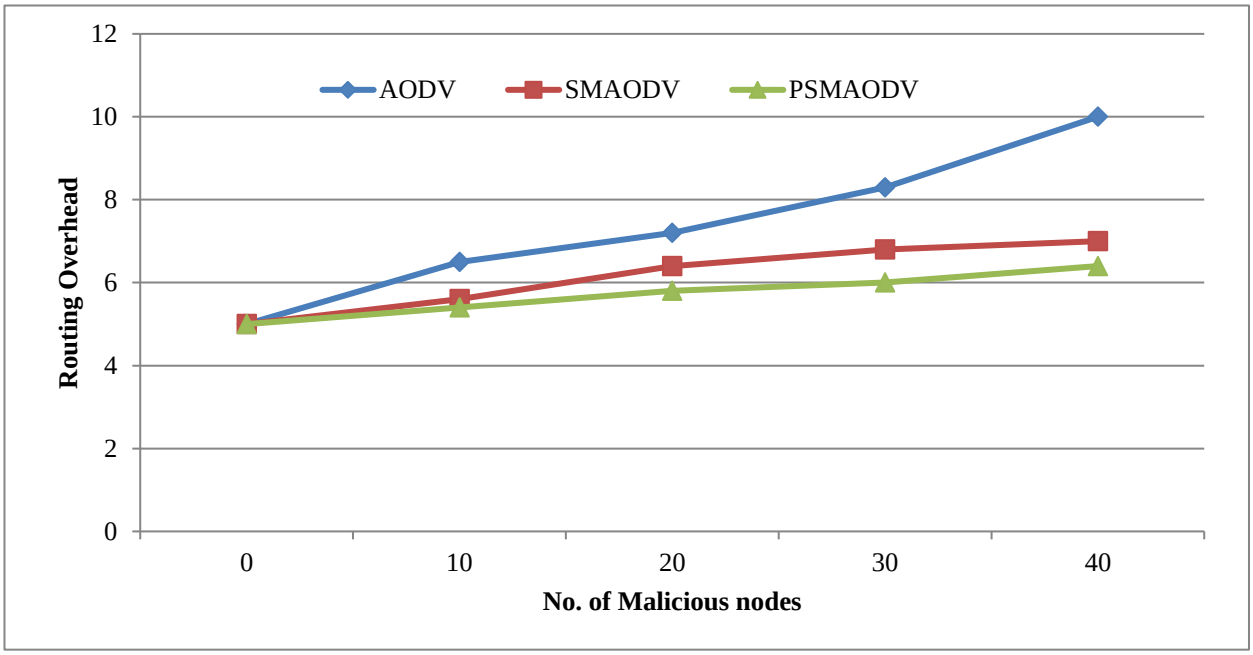

Figure 2: RO against Percentage of Malicious Nodes

Energy Consumption (EC): Figure 3 shows that Energy Consumption of AODV varies between 313 to 321 J whereas SMAODV ranges from 312 to 316 J. PSMAODV is ranges from 310 to 314 J. Thus, it shows PSMAODV has more energy efficient compared to AODV and SMAODV in different percentages of malicious nodes due to fewer route failures.

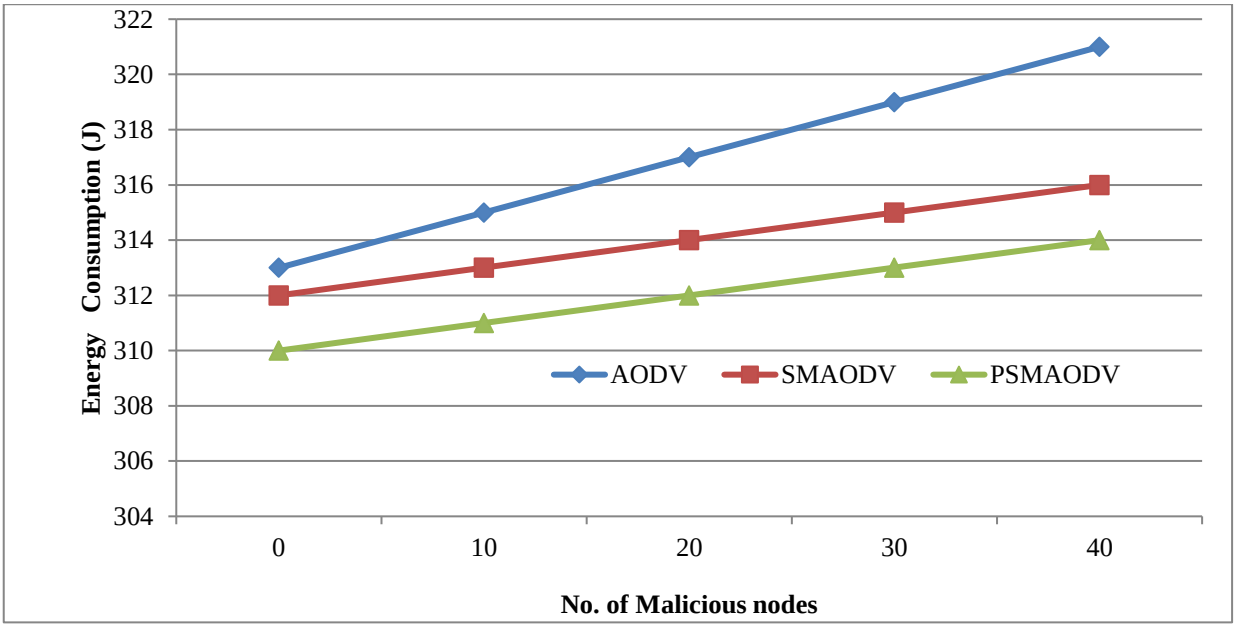

Figure 3: EC against Percentage of Malicious Nodes

5.Conclusion

This paper results that by combining trust threshold based public key management technique and the On-Demand Vector Routing Protocol, the performance and security of MANET are improved. First, CTPKM technique is included for trust threshold Key by considering three different trust dimensions, namely, competence, integrity, and social contact. CTPKM enables a node to make decisions while interacting with others based on their trust levels. Then a new parameter weight value named TLv can be used to choose the best path which ensures reliability of the path by calculating the trust value of the neighbor nodes. Also proved that the combination of trust threshold based public key management and On-Demand Vector Routing Protocol balance both performance and security.

References

[1] Zapata, M.G. and Asokan, N., 2002, September. Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security (pp. 1-10). ACM.

[2] Yang, R. and Sun, X., 2015, August. DMAODV: A MAODV-Based Multipath Routing Algorithm. In Distributed Computing and Applications for Business Engineering and Science (DCABES), 2015 14th International Symposium on (pp. 220-223). IEEE.

[3] Loganathan,P. and Purusothaman,T., 2013. An Energy Efficient Key Management and Authentication Technique for Multicasting in Ad Hoc Networks. Journal of Theoretical & Applied Information Technology, 53(1),(pp.54-62).

[4] Gowda, S.R. and Hiremath, P.S., 2013. Review of security approaches in routing protocol in mobile adhoc network. International Journal of Computer Science Issues (IJCSI), 10(1), (pp.242-251).

[5] Borkar, G.M., Mahajan, A.R. and Jawade, P., 2017, Trust Based Secure Optimal Route Selection and Enhancing QoS in Mobile Ad-Hoc Networks Using AOMDV-SAPTV and DE-Algorithm, IOSR Journal of Computer Engineering (IOSR-JCE),(pp. 55-62).

[6] Younis, M., Farrag, O. and Althouse, B., 2012. TAM: A tiered authentication of multicast protocol for ad-hoc networks. IEEE Transactions on Network and Service Management, 9(1), pp.100-113.

[7] Hu, Y.C., Perrig, A. and Johnson, D.B., 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless networks, 11(1-2), pp.21-38.

[8] Curtmola, R. and Nita-Rotaru, C., 2007, June. BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks. In Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on (pp. 263-272). IEEE.

[9] Vedhavarshini, R. and Anand, T., 2014. Efficient Data Packet Transmission in MANET using Enhanced Hybrid Cryptographic Technique. International Journal of Computer Science and Information Technologies (IJCSIT), 5(3), pp.3309-3311.

[10] Zamani, A.T. and Zubair, S., 2014. Key management scheme in mobile Ad Hoc networks. *International Journal of Emerging Research in Management &Technology*, *3*(4), pp.157-165.

[11] Zamani, A. and Zubair, S., 2014. Secure and efficient key management scheme in MANETs. *OSR J. Comput. Eng*, *16*, pp.146-158.

[12] Du, D. and Xiong, H., 2011, July. A dynamic key management scheme for MANETs. In *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011* (Vol. 1, pp. 779-783). IEEE.

[13] Jabbar, W.A., Ismail, M., Nordin, R. and Arif, S., 2017. Power-efficient routing schemes for MANETs: a survey and open issues. *Wireless Networks*, *23*(6), pp.1917-1952.

[14] Dangi, A. and Tiwari, M.K., 2016. A Secure Hybrid Communication Approach for Disaster Recovery System in MANETS. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, *5*(1), pp.PP-001.

[15] Singhi, N. and Pippal, R.S., 2018. Analysis of Key Management Schemes in MANET. *International Journal of Applied Environmental Sciences*, *13*(2), pp.161-169.

[16] Ayman, E.S., 2014. A new hierarchical group key management based on clustering scheme for mobile ad hoc networks. *IJACSA) International Journal of Advanced Computer Science and Applications*, *5*(4).

[17] Wu, B., Wu, J. and Dong, Y., 2009. An efficient group key management scheme for mobile ad hoc networks. *International Journal of Security and Networks*, *4*(1-2), pp.125-134.

[18] Cho, J.H., Chan, K.S. and Chen, I.R., 2013, March. Composite trust-based public key management in mobile ad hoc networks. In *Proceedings of the 28th annual ACM symposium on applied computing* (pp. 1949-1956). ACM.

[19] Hamouid, K. and Adi, K., 2010. Secure and robust threshold key management (SRKM) scheme for ad hoc networks. *Security and communication networks*, *3*(6), pp.517-534.

[20] Gomathi, K. and Parvathavarthini, B., 2010, December. An efficient cluster based key management scheme for MANET with authentication. In *Trendz in Information Sciences & Computing (TISC), 2010* (pp. 202-205). IEEE.

[21] Capkun, S., Buttyán, L. and Hubaux, J.P., 2003. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on mobile computing*, (1), pp.52-64.

[22] Rhee, K.H., Park, Y.H. and Tsudik, G., 2004. An architecture for key management in hierarchical mobile ad-hoc networks. *Journal of Communications and Networks*, *6*(2), pp.156-162.

[23] Pužar, M., Andersson, J., Plagemann, T. and Roudier, Y., 2005, July. Skimpy: A simple key management protocol for manets in emergency and rescue operations. In *European Workshop on Security in Ad-hoc and Sensor Networks* (pp. 14-26). Springer, Berlin, Heidelberg.