ROUTING SECURITY IN MOBILE ADHOC NETWORKS (MANETS) USING DYNAMIC ENCRYPTION

Y.Vainika[1], L. RaghavenderRaju[2], S. Navyasri[3]
[1,3]UG Student, [2]Assistant Professor
Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India.

***Abstract*--** Mobile Ad hoc Network is a collection of wireless mobile devices with restricted broadcast range and resources. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between nodes. Discovery of such routes is a major task, both from efficiency and security point of view. Due to MANET characteristics security is a key issue in ad hoc networks In this paper, we proposed a method SDE (Secure Dynamic Encryption) based on asymmetric key and dynamic encryption for the OLSR protocol. SDE-OLSR aims to enhance the security against all kinds of attacks without having impact on the performance of the network. This proposed SDE_OLSR is compared with OLSR protocol in different modes such as normal mode, attack mode to evaluate the efficiency of SDE-OLSR in MANET. This empirical results shows the increase of packet delivery rate (PDR) is by 23 % and reduction in delay by 27 %.

***Index Terms*-- OLSR, security, cryptography, dynamic keys, performance.**

I. INTRODUCTION

MANET (Mobile Ad hoc Network) is self-organizing and self-configuring multi-hop wireless network where the structure of the network changes dynamically due to mobility of the nodes. MANET is infrastructure-less dynamic network. It consists of collection of wireless nodes and the communication between these nodes are carried out without any centralized authority. Ad hoc network requires high security because, if ad hoc network is not secured properly, it allows unauthorized users to modify or disrupt or steal the data which is under transmission in the network. To secure ad hoc networks, firstly we have to study and recognize vulnerabilities in the systems which may leads to attacks, process of information exchange the network. Next, we have to use protocols which make data transmission in more secured way by reducing attacks.

Fig 1 Structure of MANET

II. RELATED WORK

Adel Echchaachoui et.al, [1] proposed a new encryption mechanism which is introduced in OLSR proactive protocol to provide high-level security for data transmission without decreasing network performance. However, this approach doesn’t have much impact reducing delay and increasing packet transmission rate.

J. Yuseok et.al [2] proposed an LT-OLSR protocol that broadcasts HELLO messages to neighbors within two-hops to defend neighbors against “Link Spoofing” attacks. This approach doesn’t have major effect on routing performance but its safety is not efficient to reject major attacks.

J. Ben-Othman et.al [3] proposed a security schema for the Radio Aware Optimized Link State Routing(RA-OLSR) protocol by applying mechanisms based on IDE. This method provides very high level of security. However, it has a significant impact on traffic performance.

R. Venkataraman et.al[4] the main objective of this study is to propose a generalized trust-model over reacting protocols in mobile ad hoc networks. It offers a good routing performance in a highly attacked environment but it doesn’t provide high levels of security especially against very complex attack.

This model brings a very interesting vision in the field of security routing in mobile Ad-hoc networks. It offers a good routing performance in a highly attacked environment but it doesn't provide high levels of security especially against very complex attacks.

III. ANALYSIS OF VULNERABILITIES AND ATTACKS

Problem Definition Based on our study and comparison of several types of attacks such as traffic analysis [3], Black-hole [11], Grey-hole [12], at the routing layer in a MANET are Denial of service i.e., DOS, such as black-hole and distributed node isolation, warm-hole, invisible node, and byzantine have shown that most ferocious denial of service attacks i.e., DDOS [17]. Our work to protect the data transmission from these attacks by using secured routing protocol OLSR.

IV. PROPOSED WORK

Approach

Our work is based on the principle of encrypting the data using public and private (Asymmetric) keys. The actuality of this mechanism is using non-centralized distribution to get dynamic keys.

Principle

The asymmetric encryption operation is based on two modes. They are:

- Generating both private and public key : In this mode each node generates their own key pairs.
- Distribution of public keys : To minimize the load of the network, we use a model based on clustering system principle. The overall network divides into groups, where in each group, a node is elected as the head of the cluster (group) and it stores all the public keys of nodes.

Operations

For electing the cluster head, each node "M" calculates and generates two keys (public and private). A private key "PKM" stores in its memory and a public key "UKM" which sends to its head of the cluster(HC).So, HC contains the list of all public keys of all the nodes present in the particular cluster. If suppose source node S wants to send the message to the destination node D, firstly it sends message to the HC for requesting the public key of destination(UKD). If D and S are present in the same cluster, HC sends public key to S, where it will encrypt the message with UKD before sending to it to D which will use its own private key for decrypting the message.

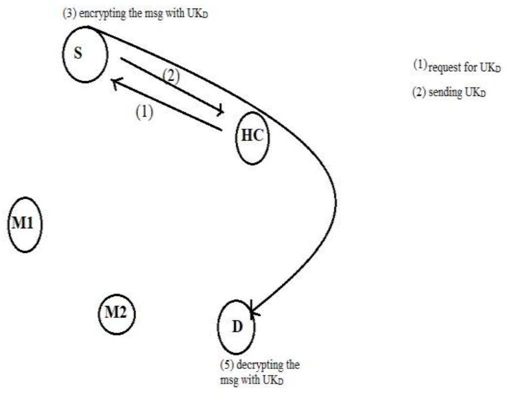
(3) encrypting the msg with UK$_D$
S
(2)
(1)
HC
(1)request for UK$_D$
(2) sending UK$_D$
M1
M2
D
(5) decrypting the msg with UK$_D$

Fig.2. Encryption in the same cluster

Else, HC uses the gateways to request the public key of the destination(UKD)at the cluster head containing D, and then sends to S. Then, message gets encrypted by the S with this key and it sends the encrypted message to the D, where decryption of the message is done by using private key "PKN ".

Public key of the node gets destroyed in the database of the HC when it leaves the cluster. It should recalculate its key pair and send the OK message to the new cluster head.

If head of the cluster changes, all nodes must recalculate and change their key pairs. After selecting the new head of the cluster the process get repeated.

Our approach uses asymmetric and dynamic encryption for messages in the network structure and offers high security routing without having delay and increases packet delivery ratio.

V. PERFORMANCE EVALUATION

For evaluating the efficiency of the SDE-OLSR system, we deployed GLOMOSIM tool. Simulation environment is created by generating a attack(DDOS) and four metrics are used to measure and compare the performance of SDE-OLSR and OLSR. The performance metric that are used in our simulations are: Packet Delivery Rate (PDR) and Delay.

A. **Simulation Process:** The attack that we deployed in our simulations is DDOS. To know the effect of our security mechanism on performance of the network i.e., Effectiveness of proposed encryption system against spoofing and taking control of the data we performed simulations where we evaluated SDE-OLSR under DDOS attack.

Table.1. Simulation Parameters

PARAMETERS	VALUES
Area	1000m * 1000m
Speed	0-40 m/s
Pause time	0 s
Simulation time	300 s
Number of nodes	1-100
Number of pairs(connections)	10
Mobility model	RWP

B. Simulation Result

PDR: Under DDOS attack, the PDR of OLSR and OLSR-SDE decreased considerably, respectively, by 68 to 35% and by 81 to 42%, with the increase of the density of the network. These measurements indicate that the rate of delivery of packets, under DDOS attack, increased by 82% for the OLSR, while it increased by only 56% for OLSR-SDK. Due to its security mechanism and the rejection of infected packets, the OLSR-SDK allowed the increment in PDR by 23%. We found similar results when we measured, in the three cases, the number of packets lost in relation to the mobility of nodes. Fig.8. We concludes that mobility has not an impact on our protocol.

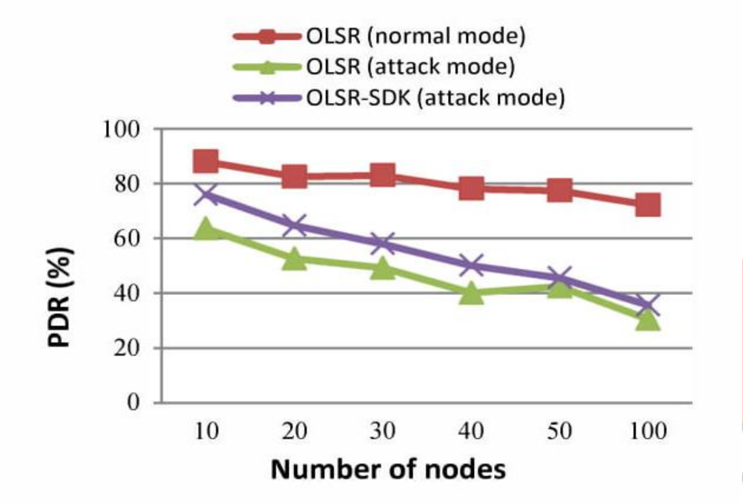

Fig.3. Packet loss under DDOS attack, relative to the mobility

End-to-end delay: In relation to the mobiliy of the network, the delay of the OLSR, in normal mode, continuously increase from 1 to 36ms. Under DDOS attack, the delay of OLSR and OLSR-SDE increases, respectively, from 5 to 62ms and from 52 to 1.5ms, when the number of nodes increases from 10 to 100. Fig. Therefore, the delay of the OLSR increased by 131%, while that of OLSR-SDE increased by only 63%. Despite the necessary and additional time that our mechanism of security uses to encrypt the data and to disrupt the infected packets, OLSR-SDE has reduced the time of transmission by 22%.

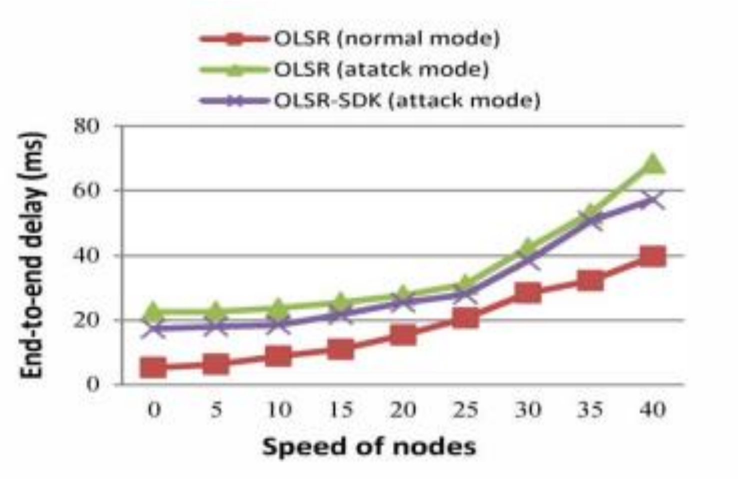

Fig.4. End-to-end delay under DDOS, relative to the mobility

However, we have noticed a slight increase in the gap between OLSR and OLSR-SDE (27% instead of 22%), because when the speed of the nodes increases, the transmission delays automatically increases because the time required to process the security mechanism gets increased.

VI. CONCLUSION AND FUTURE WORK

In this paper we implemented a new approach which is able to combine the high security and the high performances in the routing process of Ad-hoc networks. We used a principle of encryption based on asymmetric key and dynamic cryptography and a Key Distribution is managed by clustering organization, and we implemented this mechanism in a protocol called OLSR-SDE, which is based on OLSR. Our study about types of attacks and their criticality levels, allowed us to select an deadly attack for our simulations: DDOS. The empirical results we obtained in comparison with standard OLSR, showed that OLSR-SDE, providing a high level of security, has greatly improved traffic performance (23% improvement in PDR and 27% improvement in delay) against an DDOS attack that directly target nodes. To improve our security system, we will work on a new approach that, in addition to securing content, must resist to data destruction attacks.

REFERENCES

[1] Adel Echchaachoui, Ali Choukri, Ahmed Habbani and Mohamed Elkoutbi :”Asymmetric and dynamic encryption for routing security in MANETS.

[2] 1. Yuseok, K. Tae-Hyung, K. Yuna, and K. Jong, "LTOLSR: Attack-tolerant OLSR against link spoofing, " in Local Computer Networks (LCN), 2012 IEEE 37th Conference on, 2012, pp. 216-219.

[3] J. Ben-Othman and Y. I. S. Benitez, "A new method to secure RA-OLSR using IBE, " in Global Communications Conference (GLOBECOM), 20i2 iEEE, 2012, pp. 354-358.

[4] R. Venkataraman, M. Pushpalatha, and T. Rama Rao, "Regression-based trust model for mobile ad hoc networks, " Information Security, lET, vol. 6, pp. 131-140, 2012.

[5] R. K. Singh, R. Joshi, and M. Singhal, "Article: Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET), " International Journal of Computer Applications, vol. 68, pp. 25-29, April 2013.

[6] P. M. Jawandhiya and M. M. Ghonge. A Survey of Mobile Ad Hoc Network Attacks.

[7] M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks, " Communications and Networks, Journal oj, vol. 15, pp. 31-37, 2013.

[8] Garci, x, L. 1. a Villalba, 1. Garcia Matesanz, Rupe, C. rez, xOOF, D. as, and A. 1. Sandoval Orozco, "Secure extension to the optimised link state routing protocol, " Information Security, lET, vol. 5, pp. 163-169, 2011.

[9] P. Jacquet and T. Clausen, Optimized Link State Routing Protocol (OLSR): RFC Editor 3626, 2003.

[10] A. Nadeem and M. Howarth, "A Survey of MANET Intrusion Detection &amp; Prevention Approaches for Network Layer Attacks, " Communications Surveys & Tutorials, IEEE, vol. PP, pp. 1-19, 2013.

[11] U. Venkanna and R. 1. Velusamy, "Black hole attack and their counter measure based on trust management in manet: A survey, " in Advances in Recent Technologies in Communication and Computing (ARTCom 2011), 3rd International Conference on, 2011, pp. 232-236.

[12] G. Usha and S. Bose, "Impact of Gray hole attack on adhoc networks, " in Information Communication and Embedded Systems (ICICES), 2013 International Conference on, 2013, pp. 404-409.

[13] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc networks, " in Computer Networks, 2006 International Symposium on, 2006, pp. 30-35.

[14] M. Sadeghi and S. Yahya, "Analysis of Wormhole attack on MANETs using different MANET routing protocols, " in Ubiquitous and Future Networks (ICUFN), 2012 Fourth international Conference on, 2012, pp. 301-305.

[15] S. Agrawal and S. Jain, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, " JOURNAL OF COMPUTING, vol. 3, January 2011.

[16] K. S. Chan and M. R. Alam, "TCBWD: Topological comparison-based Byzantine wormhole detection for MANET, " in Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on, 2011, pp. 388-394.

[17] S. T. Zargar, 1. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, " Communications Surveys & Tutorials, IEEE, vol. PP, pp. 1-24, 2013.

[18] A. Choukri, A. Habbani, and M. El Koutbi, "Eflicient Heuristic Based on Clustering Approach for OLSR, " Journal of Computer Networks and Communications, vol.2013, p. 7, 2013.

[19] 1.-P. Aumasson, O. Dunkelman, S. Indesteege, and B.Preneel, "Cryptanalysis of Dynamic SHA(2), " in Selected Areas in Cryptography. vol. 5867, M. Jacobson, Jr., V.Rijmen, and R. Safavi-Naini, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 415-432.