ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Secure and Optimizing Routing Technique for MANETs

Komal Khedkar

M.E. Student, Dept. of C.E., D.P.C.O.E. Wagholi, Pune, Maharashtra, India

ABSTRACT: Mobile ad hoc network (MANET) is a self-organizing, dynamic topology network formed by a collection of mobile nodes connected without wires. Network is not secure due to the mobility and dynamic nature of MANET. Because of its characteristics, it is more vulnerable to different types of attacks and security threats. So network should be secure against attackers. In MANET on demand routing protocols provide cost effective and scalable solutions for packet routing but the path generated by these protocols may deviate far from the optimal path because of the lack of knowledge about the global topology and the mobility of nodes. Routing optimality also affects network performance and energy consumption. In this work we propose efficient secure routing localized key management (ESR-LKM) protocol which can optimize the path dynamically to enhance performance and reduce energy consumption. The proposed path aware ESR-LKM algorithm finds the shortest path by reducing the number of hops. And to prevent attackers efficient key management and cryptography is used.

KEYWORDS: Mobile Ad hoc network (MANET), Security, Routing, Key Management.

I. INTRODUCTION

Mobile ad hoc network is infrastructure less, self-configuring, dynamic topology network formed by a collection of mobile nodes through radio links. Each node of MANET acts as a sender, receiver and sometimes as a router. Intermediate nodes may cause several problems during data transmission session like it can drop packets, deny to forward packets or may modify the contents of packets. Such nodes are called as malicious nodes. This can be prevented by using cryptography.

Distant nodes intercommunicate through multi-hop paths because mobile nodes have limited transmission capacity. The lack of the need of any infrastructure and the ease of deployment makes MANETs an attractive choice for a variety of applications like in disaster recovery, communications in battle ground and for interactive information sharing in remote areas. Low transmission power, continuously changing network topology and low available bandwidth are major challenges for routing in MANETs. So routing protocols should adjust to network topology changes and should not incur too much overhead in terms of the transmission of control messages.

With the increase in the average route length and size, scalability becomes a major issue for the current ad hoc routing protocols. Proactive routing protocols that require periodic advertisement and global dissemination of connectivity information are not suitable for large networks. Reactive protocols maintain the route that are currently needed by initiating a path discovery process whenever a route is needed for message transfer, so these protocols are efficient for routing in large ad hoc networks.

Our approach can be summarized as, for any given routing path between source and destination, how can we optimize the path dynamically to enhance performance and reduce energy consumption. So in this work we proposed one path aware efficientsecure routing localized key management protocol (ESR-LKM) which optimizes path dynamically as well as provides security against attackers.

II. RELATED WORK

The SR-LKM protocol [1] uses a localized key management mechanism and in this a network node performs all key management activities within its one hop neighborhood only. This protocol is free from key management – secure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

routing interdependency problem because the localized key management approach used in this protocol is independent on any secure routing protocol. For broadcast key distribution, it uses the LCM based broadcast key distribution mechanism. It can prevent both inside and outside attackers with the help of a monitoring based revocation mechanism. Its per node storage requirement is not dependent on the total number of nodes in the network so it is storage scalable. The drawback of this protocol is that it assumes an offline CA existing outside the network which distributes the PKCs to all the nodes in the network. But if the CA is not trusted then the network is not secure.

SE- AODV [2] uses symmetric key cryptography for authenticating routing control packets. SE- AODV adds extra features to same AODV routing protocol and makes path formation more secure. In this a GTK encrypted with PTKs is distributed by each node to all of its neighbors, so such key bandwidth mechanism is highly bandwidth consuming.

In AODV [3] a novel algorithm for finding the on demand route is proposed. In this each mobile host operates as a specialized router and routes are obtained as needed with little or no reliance on periodic advertisements. It provides loop – free routes even while repairing broken links. Because it does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements. The drawback of this protocol is that it only used for efficient path formation but there is no concern for security.

GSBRA [4] divides the network into small grid zone. To route data it utilizes PGH and BGH chains. The BGH works as a backup for the PGH and is a future leader for the grid. The backup route can be established through the BGHs and the primary route can be established through the PGHs. It improves the network lifetime but does not consider the path optimization.

ARANz [5] increases security, achieve robustness and solve the single point of failure and attack problems by introducing multiple local certificate authority servers. The drawback of this protocol is that it does not consider topology changes, path optimization etc.

DR-AODV [6] computes routing path with the lowest delay while providing resilience and fast reverse route discovery when subjected to unidirectional links. It performance well in scenarios where the numbers of unidirectional links are exceptionally high. It is used only for efficient path formation but does not consider security issues in MANET, so it is not suitable for malicious free path formation.

In Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique [7] an efficient clustering scheme for application level multicast key distribution in mobile ad hoc networks is presented. They showed that their scheme can be combined with the Multipoint Relaying technique in a very effective way according to the localization of the group members and their mobility. But key distribution reliability is not considered in this paper.

In MP-DSR: A QoS-aware Multi-path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks [8] they proposed multi-path dynamic source routing protocol to provide data transmission with higher end-to-end reliability in wireless ad hoc networks. This protocol forwards outgoing packets along multiple paths that are subject to a particular end-to-end reliability requirement. The drawback of this protocol is that it does not provide any mechanism to prevent inside attackers.

In [9] a co-operative security scheme called Reliable Ad hoc On-demand Distance Vector (RAODV) routing protocol based on local monitoring is proposed to solve the problem of attack by malicious node as well as selfish behavior. RAODV behaves as AODV in the absence of attack and detects and isolates misbehaving nodes in the presence of attack. Also it recovers from the attack when a misbehaving node leaves the network or becomes good**.** In absence of attacks it only finds on demand routes but does not finds shortest route.

In Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet [10] a light weight solution for secure routing is proposed. Proposed protocol IBC-based secure global AODV (IGAODV) uses IBC to avoid certificates and MIC & tokens to minimize the computational overhead. IGAODV is resistant to most common security attacks such as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

modification, fabrication, replay attacks and it can also protect hop count. IGAODV is not resistant to collaborative, black hole, and gray hole attacks.

III. PROBLEM DEFINITION

Mobile Ad hoc network (MANET) is a continuously infrastructure-less, self-configuring network of mobile devices connected without wires. Each and every device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. Each device must forward traffic unrelated to its own use and therefore be a router. Routing protocol addressed for only efficient path formation makes the same network vulnerable to various types of attacks. Packets that are routed during route discovery process need to be protected in such a way that it has a least probability of having a malicious node in path formed.

Paths longer than the shortest available paths are also not desirable because extra bandwidth is consumed and end-to-end delay is long. So it is necessary to optimize the path dynamically between source and destination to enhance performance, reduce energy consumption and to secure network against attackers.

IV. PROPOSED SOLUTION

The proposed efficient secure routing using localized key management (ESR-LKM) address these issues of security and route formation in MANET. In this work we proposed one path aware ESR-LKM algorithm which optimize the path dynamically to enhance performance and reduce energy consumption. In this ESR-LKM, a network node performs all key management activities such as key establishment, renewal and revocation. So the ESR-LKM mechanism is not dependent on any routing protocol and it does not suffer from the key management secure routing interdependency problem. To prevent attackers cryptography is used. Different phases of proposed work are shown below in figure 1.

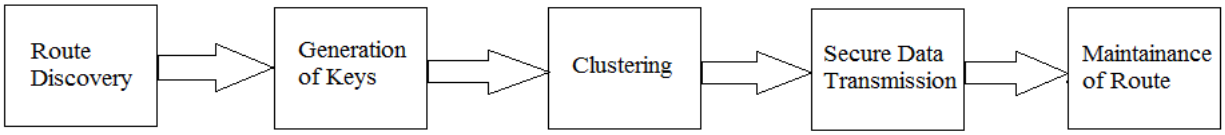

Figure 1. Different Phases included in Proposed Work

V. PROPOSED ALGORITHM

Path aware ESR-LKM:

When node i overhears a packet P,
BEGIN:
Step1: If the node i is the destination node
Then consume the packet. GOTO END;
Step 2: (Assume packet P belong to (S_x, D_x) flow.)
Compare (S_x, D_x) with all the valid entries in the hop comparison array;
Step 3: If there is no match with the entries,
Store (S_x, D_x, HC_x, N_x) in the hop comparison array;
Step 4: If the packet is destined to I as the next-hop node, process the packet for forwarding further. GOTO END;
Step 5: (Assume that it matched with an entry (S_x, D_x, HC_y, N_y)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

If ((HC_x – HC_y) > 2)
Short-cut is found. Node I does the following steps:
Step 5.1: Send a message to N_y to update the routing table such that the next hop address for destination node D_x is modified to the address of node I;
Step 5.2: Modify its routing table by making the next-hop address for destination D_x as N_x
Step 5.3: Modify its hop comparison array, delete the entry corresponding to (S_x, D_x);
END

VI. MATHEMATICAL MODEL

Let S be the system that describes source packet as input to the system with path-aware ESR-LKM, node monitoring mechanism and clustering; this all gives output as short-cut path discovery . Figure 2 shows illustration of mathematical model for the proposed system.

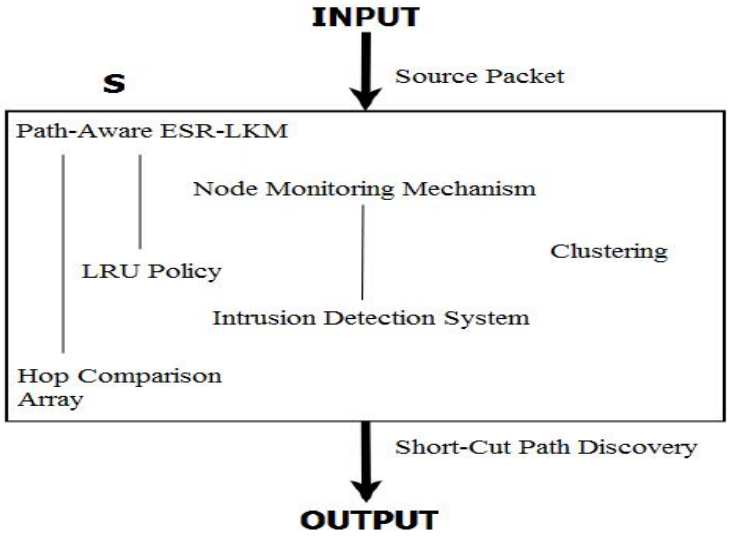

Figure 2. Illustration of Mathematical Model

S = (S_x, route-chk, D_x)

Where S = system,
S_x = Source node,
route-chk = check source node has any destination node,
D_x= Destination node

INPUT
S_x = source packet

Path Aware ESR-LKM
Hop comparison array = (S_x, D_x, HC_x, N_x)
where
S_x = Source address,
D_x = Desination address,
HC_x = Hop counter,
N_x = Neighbors address,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

LRU Policy = If hop comparison array becomes full with valid entries then new entries can replace older entries using the least-recently used algorithm (LRU) policy

Clustering:
The nodes are divided into number of clusters
Node Monitoring Mechanism
In node monitoring mechanism, each node monitors the routing behavior of all its neighboring nodes

Output
The output is the short- cut path discovery.

VII. EXPERIMENTAL RESULTS

The work done results are shown in figures given below. Figure 3 shows the output screen for nodes in the network and a connection among them.

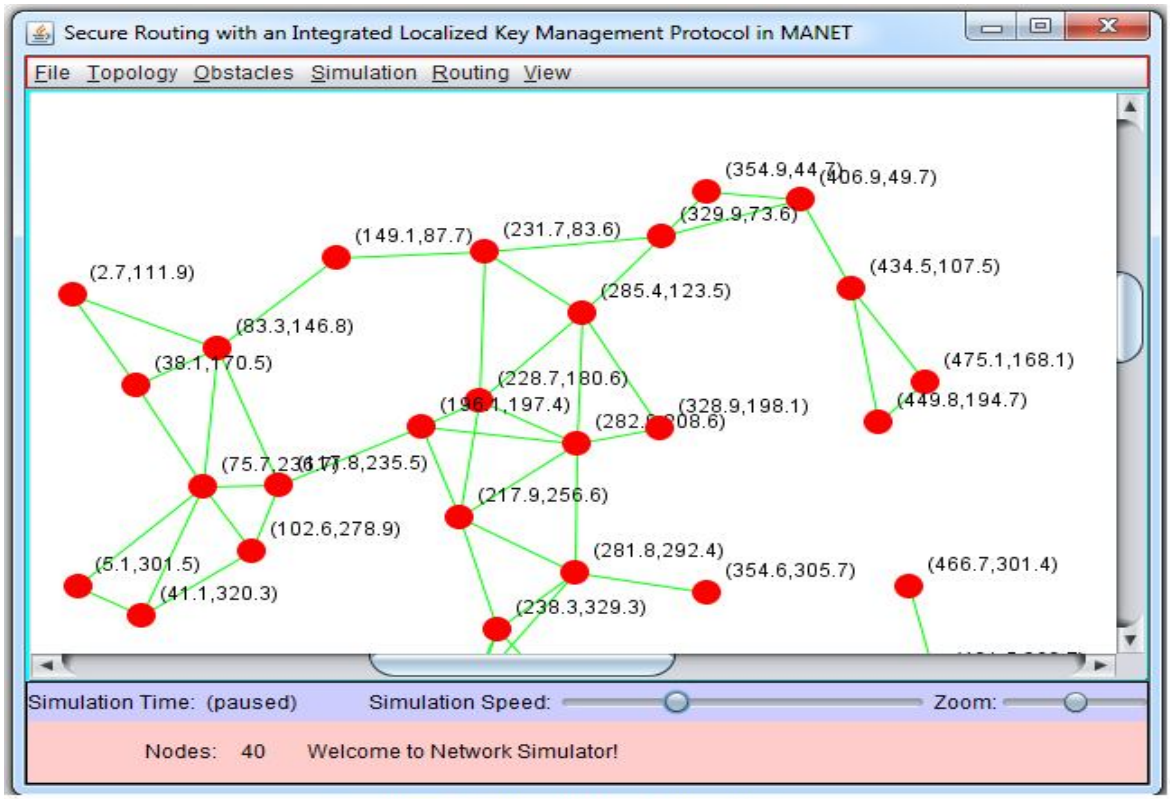

Figure 3. Nodes in the Network

Figure 4. shows the energy graph for the existing and proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

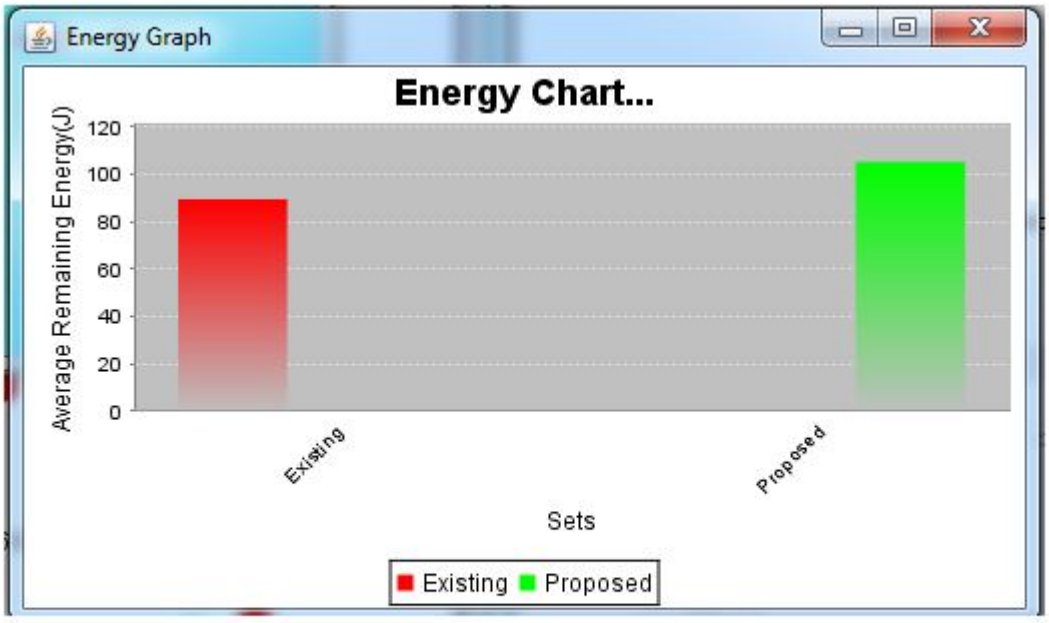

Figure 4. Energy Graph

VIII. CONCLUSION AND FUTURE SCOPE

MANET is a collection of independent nodes and via bidirectional links these nodes can communicate with each other. In this paper, we proposed a path aware ESR-LKM of self-hiding and optimizing routing technique for mobile ad hoc networks. It improves routing optimality by monitoring routing paths continuously and gradually redirecting the path towards a currently more optimal one. The basic idea is to let neighboring nodes of a routing path together with the on-route nodes, monitor the route so that up-to-date information about relative local topology and link quality is exploited. When more optimal sub path occurs and is estimated to be stable, it will be utilized to redirect the route. Unlike many of the existing authentication based secure routing protocols, the proposed protocol can prevent inside attackers also.

In future, further research can be done to find the best possible optimal routing approach which will be more secure and promising in terms of energy efficiency.

IX. ACKNOWLEDGEMENTS

Sincere thank to the reviewers for reviewing this manuscript and providing inputs for greatly improving the quality of this paper.

REFERENCES

1. Shrikant H. Talwar, SumyadevMaity and R.C. Hansdah, “Secure Routing with an integrated localized key management protocol in MANETs”, International Conference on Advanced Information Networking and Applications, pp. 605-612, 2014.
2. Rajdeep S. Shaktawat, Dharm Singh, Naveen Choudhary, “An Efficient Secure Routing Protocol in MANET Security-Enhanced AODV (SE-AODV)”, International Journal of Computer Applications, vol.97, no.8, pp. 34-41.
3. C. E. Perkins and E. M. Royer, “Ad-hoc On-Demand Distance Vector Routing”, Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, Feb. 1999.
4. Zhengyu Wu, Hantao Song, Shaofeng Jiang, XiaomeiXu, “A Grid-based Stable Backup Routing Algorithm in MANETs”, International Conference on Multimedia and Ubiquitous Engineering, 2007.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

5. Liana KhamisQabajeh, Dr. Miss Laiha Mat Kiah, Mohammad MoustafaQabajeh, "A Scalable Secure Routing Protocol for MANETs", International Conference on Computer Technology and Development, pp. 143-147, 2009.
6. Megat F. Zuhairi, David A. Harle, "Dynamic Reverse Route in Ad hoc on Demand Distance Vector Routing Protocol", Sixth International Conference on Wireless and Mobile Communications, pp. 139-144, 2010.
7. Mohamed Salah Bouassida, Isabelle Chrisment, Olivier Festor, "Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique", Proceedings of the International Conference on Networking, pp. 1-7, 2006.
8. Roy Leung, Jilei Liu, Edmond Poon, Ah-Lot Charles Chan, Baochun Li, "MP-DSR: A QoS-aware Multi-path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks", Proceedings of the 26th Annual IEEE Conference on Local Computer Networks, pp. 1-10, 2001.
9. SandhyaKhurana, Neelima Gupta, NagenderAneja, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol", International Conference on Mobile Communications and Learning Technologies, pp. 1-6, 2006.
10. K. Ramanarayana, Lillykutty Jacob, "Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet", Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing, pp. 1-6, 2007.