IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Link Lifetime Prediction and Secure Data Transmission in Mobile Adhoc Network

Ashish Kumar Awadhiya[1], Prof. Rohit Vyas[2], H.O.D .Vivek Sharma[3]

Technocrats Institute of Technology College, Bhopal, M.P. India[1, 2, 3]

Abstract: MANET is a system which workings on idea of having network short of any setup. MANET’s having number of node demands high quality of processing power, high bandwidth and memory to provide definite routing information, though induces traffic overhead in the mobile network. DSR protocol is a sensible protocol in MANET. Due to the intrinsically self-motivated nature of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. Nodes mobility has greatest impact on available routes. Mobility leads to dynamic topologies of the network which enforces nodes to update their neighbor information and associated routes to a node. Different routing protocols update this information in different ways. Determination of link lifetime, data security, detection of malicious node and secure information transmission in a MANET is an important tasks in any mobile network. Our proposed protocol discover the link lifetime and if original link is breakdown then new secure node is established and information is transferred from newly created link. We proposed a secure trust value which helps authenticate the node and also keep safe the network from malicious nodes. The system also perform secure routing to protect MANET against malicious node. Experimentally result showed that our scheme is well suited for better data transmission. The simulation results discovered that the data delivery percentage and performance of the system is improved.

Keywords: MANET, Routing, Security, Link lifetime, Multihop network

I. INTRODUCTION

Digital information are growing using the networks of mobile devices anywhere at any time and becoming the need of today. Without using some static structural support the info is transferring in the setup of mobile devices. This type of networks is called as ad –hoc network. To set up the network for the nodes for short period of time is objective of the of ad-hoc network. MANET is a setup which workings on idea of having network without any static infrastructure. Such network consists of mobile nodes which are free to move. They come together for a span of time for give and take process means to receive and give the information in return. All information is used by each device, can be assumed as producers and consumers in an ad-hoc network [1]. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared. Ad hoc setup reduces the requirement of static infrastructure and install the speed. Mobile devices are not having the centralized control, therefore they are free to move, and hence the topology of such network changes expeditiously. In the mobile Adhoc system, a number of influences such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the lifetime of a link among two mobile nodes. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET[2] often traverse along a path spanning multiple links, which is known as the multihop path. Detection and correction of link lifetime to increase performance and trustworthiness of mobile Adhoc network using dynamic source routing under malicious attack with secure routing and data transmission. In MANET the mobile wireless network is not rely on any existed network. It is a combination of several wireless nodes that can build a network randomly. Ad-hoc network doesn’t depend on any central administration or stable infrastructure such as base. While nodes are moving in the network they interchange the information to each other and may continue to move here and there and so the network must be prepared.

In order to detect link lifetime[1], we proposes a scheme which help in report to the MANET. And also find path to secure data transmission. We evaluate the secure value of each node using timestamp. Then to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch connection letdown.

The rest of the paper is organized as follows.

Section 2 provides the background, relevant for the context. Section 3 provides the proposed methodology, proposed algorithm and description of proposed methodology. Section 4 represents the implementation of proposed methodology, discussion on simulation Results and performance analysis of simulation results. Section 5 concludes the paper with a summary of the main findings concluding remarks, limitation discussion and an outlook on future research directions.

DOI 10.17148/IJARCCE.2016.5989

II. BACKGROUND AND LITERATURE SURVEY

2.1 Problem Identification

To achieve reliability[3] and availability, routing protocols should be powerful against both link lifetime prediction and malicious attacks. In the mobile Adhoc system, a number of effects such as physical obstacles movement, unwanted noise, and climate circumstances contribute to the trouble of precisely forming the actions of the lifetime of a link among two mobile nodes. Due to the intrinsically self-motivated nature of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. Recognition of malevolent[4] node data Security and in a MANET is an important tasks in any network. The excellence of service must fulfil source end to destination end data packet transfer without packet loss. Detection and correction of link lifetime to increase performance and trustworthiness of mobile Adhoc network using dynamic source routing under malicious attack with secure routing and data transmission. To improve the data delivery ration and performance of MANET and also detect and correct link lifetime is the main problem in MANET. Mobile Adhoc network needs safety and consistency of data packets. Real time applications in MANET require certain qualityofservice (QoS)[5] features, such as minimal end-to-end packet delay and acceptable data loss. Determination of link lifetime, data security, detection of malicious node and secure information transmission in a MANET is an important tasks in any mobile network. Detection of link lifetime of mobile nodes with the help of routing info is also problematic in an ad hoc network due to its real time altering topology. Data packets routed between a sender node (source) and a receiver node (destination) of a MANET often traverse along a path spanning multiple links, which is known as the multihop path. The objective is to detect and link lifetime of the mobile network, to improve the data delivery ration and performance of MANET, to select best route for secure data transmission. The proposed protocol discover the link lifetime and if original link is breakdown[6] then new secure node is established and information is transferred from newly created link.

2.2 Literature Survey

The concepts dynamic source routing is based on the source routing which means the initiator of the packet provides an orderly list of nodes according to which packet traverses[7] in the network. The key note this routing pattern is that intermediate nodes need not to track the information of the routing through which packet will traverse in the network as source node already has a decision regarding the routes. Utilization of source routing allows the packet to travel in the loop free environment, elude the requirements for updating the routing information in the intermediate node, allows the node to forrard the packet to store the routing information in them for future. All aspects of protocol operate entirely on demand [8]. DSR[9] works in completely self configuring and organizing without pre existence of structured network for any existing network infrastructure or administration. Route discovery is a method of finding out the secure route in the network, when a source node’s having a desire to transmit the data packet to the destination node, where every node holds a route cache of source routes it has understood or overheard. Route maintenance is the mechanism by which originator device recognize the alteration occurred in the network topology such that it understands about the longevity of the route available to the destination because of the node in the route list is moved out of the range.

DSR works a finding the route and uses that route called source route. Sender has a complete knowledge of particular sequence orders of the network nodes to reach at the destination. The initiator than pass this packet into the network interface wireless medium[10] to the first node which is identified by the route in its route cache. If that node is not the destined address, it forward the packet following by the further node mentioned in the route cache. Once after another, process is continuous, until not reached to the final destination. Route discovery is the action of finding the best path from source node to destination node done by the originator. This mechanism starts on when a source node is wish to send a packet to the destination and is not finding the best path in its route cache. In route discovery primarily the initiator node will first search the route from source to destination by utilizing its route cache. If the initiator fined the path it will start sending the packet in a transmission range by wireless medium. Route maintenance[11] is the process of maintaining the routes in network if the link failure occurred. DSR follows this mechanism to delete the broken link from the network while propagating the packet from the source to the destination. The basic concept of route maintenance in DSR is that every node is responsible for acknowledging that the next node in the source path had received the packet.

III. PROPOSED WORK

In order to detect link lifetime, we proposes a scheme which help in report to the MANET. And also find path to secure data transmission. We evaluate the secure value of each node using timestamp. Then to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch connection letdown. Our procedure guarantees that multi cast data is transported from the source to the associates of the multi cast groups, even in the presence of link letdown, as long as the group members are accessible through non adversaril track. Here authentication framework is used to remove outside adversaris and guarantee that only approved nodes accomplish certain operation.

OUR PROPOSED PROCEDURE CONTAINS SUBSEQUENT STAGES :

(1) Scenario setup, Node setup, Routing protocol setup, Source and destination setup

DOI 10.17148/IJARCCE.2016.5989

(2) Link lifetime detector gathers all links statuses on the foundation of values collected from a prior investigation of flooding process, in which hop count to reflect the in/out-going link performances.
(3) Trust key computing
(4) Secure node authentication
(5) Secure route discovery across the node.

```
Select a node to destination
Check selected node in fresh_route cache
If yes then
Route is confirmed
Else
        Select another new secured node
End if
```

(6) Backup node setup phase.
(7) Route maintenance across the node.

During flooding processes link scanner passively collects hop counts of established investigation messages at MANET nodes. Based on the surveillance that damaged links can result in disparity between received hop counts and network topology. The object of link scanner is to make available a list encompassing all possible links lifetime. With such a list, more recovery and analysis procedures become possible, including (a) altering routing policy for the related nodes, (b) discovering the root causes of observed indications in the network, (c) contribution the auxiliary list of lifetime links for every single node.

The first steps in algorithm is trust key value calculation. The dynamic assignment of weight is introduced in the network to compute a valid key which can be useful to define the consistency of neighbor node. To calculate the trust value a new trust policy has been introduced in link and network layer to calculate a valid key which can be useful to define the reliability of neighbor node, where the key calculation includes self-motivated assignment of the weights. The next step is to search for secure node authentication. Secure node authentication is necessary steps in secure data transmission. The verification framework stops untrusted nodes. The next step is the route discovery. In this step the node will find secure node to transfer data from source to destination. We have used fresh route cache to easily find the path. The next step is backup node phase. Backup nodes are the nodes which contains the different secure path if the system fails to get the secure path. Due to backup node the data can be transferred to destination. The next step is to maintain the route for secure data transmission. Damaged link detection becomes more problematic in the multi-hop networks due to topology structures.

IV IMPLEMENTATION

We used NS2 simulator for implementation of proposed work. We also used C/C++ and TCL language for implementation. We used NS2 simulator for implementation of proposed work. We also used C/C++ and TCL language for implementation. We performed our experiment in i3 3.0 GHz machine with 4GB RAM. For this simulation, we have used the network parameters, such as Dimension, Number of nodes, traffic, transmission rate, Routing protocol, transmission range, sensitivity, transmission power etc., are used. We have performed our experiment with different number of nodes, with or without mobility. The dimensional area and speed of the scenario is also changed according to situation. With the help of reverse route the node will send link damage message to the upstream node. This error message is used by node to detect link failure in the wireless sensor network.

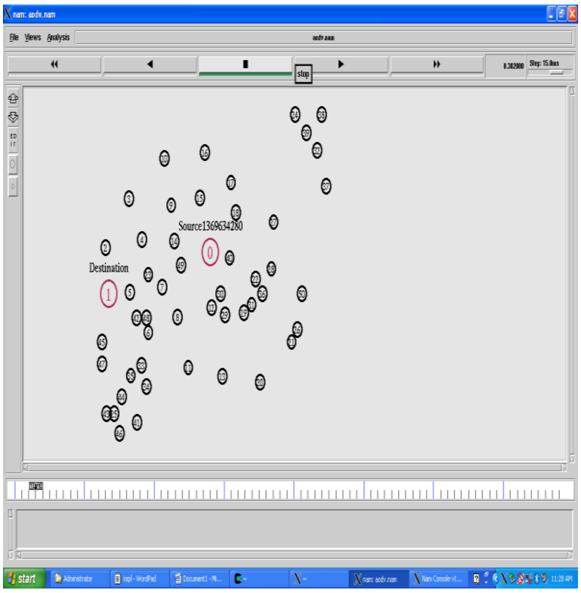
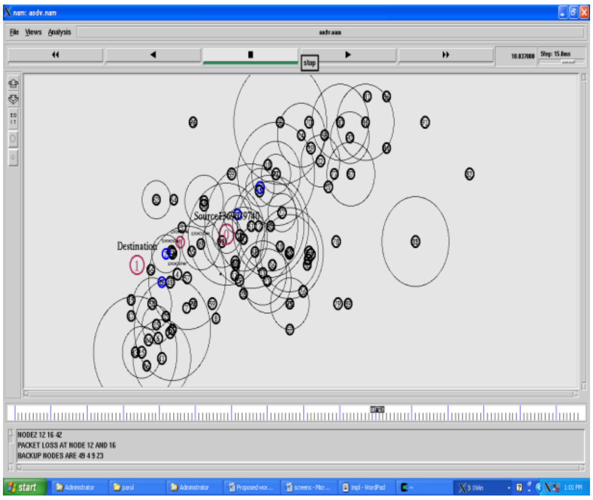


Figure 1 Simulation setup



NODE2 12 16 42
PACKET LOSS AT NODE 12 AND 16
BACKUP NODES ARE 49 4 9 23

Figure 2 Simulation result

Simulation readings of the proposed protocol are carried out to estimate its performance, and compared its performance. Fig. 2 represents the data transfer percentage of all the three routing protocols. It is noted that the data transmission ratio of all the set of rules rise as the node compactness increases. When node density is very high, there are additional nodes available for data promoting, and this rises the delivery ratio.

DOI 10.17148/IJARCCE.2016.5989

Table 1 Simulation scenario

Quantity of nodes	50, 100, 150, 200, 250, 300
Simulated area dimension	500×500
Routing Procedure	DSR
Simulation time in seconds	100
Transport Layer	FTP, TCP
Traffic flow type	CBR
Packet size in bytes	1010
Quantity of traffic links	20 , 8
Max. Speeds in m/s	30

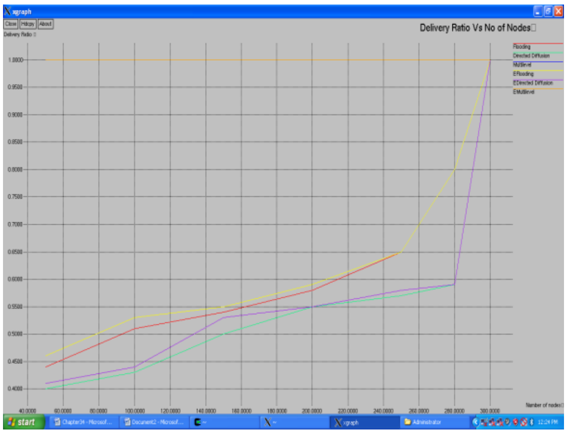


Figure 3 Performance Graph for Delivery Ratio Vs Number of Nodes

Fig. represents the data transfer percentage of all the three routing protocols. It is noted that the data transmission ratio of all the set of rules rise as the node compactness increases. When node density is very high, there are additional nodes available for data promoting, and this rises the delivery ratio. Overflowing offers less data delivery rates, followed by flooding is directed diffusion; it did not familiarize well its performance to network size growth. The multilevel routing protocol has preserved continuous transport rates throughout the simulated situations. This is an outcome of the influence of the process it uses to create a routing route.

V. CONCLUSION

MANET's having number of node demands high quality of processing power, high bandwidth and memory to provide definite routing information, though induces traffic overhead in the mobile network. Transmitting procedures of Ad-hoc network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. Due to the intrinsically self-motivated nature of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. DSR works in completely self configuring and organizing without pre-existence of structured network for some current system administration and infrastructure. DSR works a finding the route and uses that route called source route. Recognition of malevolent node data Security and in a MANET is an important tasks in any network. We proposed a secure trust value which helps authenticate the node and also keep safe the network from malicious nodes. Determination of link lifetime, data security, detection of malicious node and secure information transmission in a MANET is an important tasks in any mobile network. Our proposed protocol discover the link lifetime and if original link is breakdown then new secure node is established and information is transferred from newly created link. The system also perform secure routing to protect MANET against malicious node. Experimentally result showed that our scheme is well suited for better data transmission. The system also perform secure routing to protect MANET against malicious node. The simulation outcomes discovered that the data delivery ratio and overall performance of the system is improved.

REFERENCES

[1] Edward Y. Hua, and Zygmunt J. Haas, Mobile-Projected Trajectory Algorithm With Velocity-Change Detection for Predicting Residual Link Lifetime in MANET, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 64, NO. 3, MARCH 2015, pp-1065-1079

[2] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for AdHoc network research," Wireless Commun. Mobile Comput. Special Issue Mobile Ad Hoc Netw.: Res., Trends, Appl., vol. 2, no. 5, pp. 483–502, Aug. 2002.

[3] S. S. Ahuja, S. Ramasubramanian, and M. M. Krunz, "Single-link failure detection in all-optical networks using monitoring cycles and paths," IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[4] Edward Y. Hua and Zygmunt J. Haas," Mobile-Projected Trajectory Algorithm With Velocity-Change Detection for Predicting Residual Link Lifetime in MANET", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 64, NO. 3, 2015, pp. 1065-1079

[5] A. Cerpa, J. L. Wong, L. Kuang, M. Potkonjak, and D. Estrin, "Statistical model of lossy links in wireless sensor networks," in Proc. IEEE IPSN, 2005, pp. 81–88.

[6] Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link Detection for Wireless Sensor Networks, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 14, pp 4428-4438, Aug 2015

[7] R. Korsnes, K. Ovsthus, F. Y. Li, L. Landmark, and O. Kure, "Link lifetime prediction for optimal routing in mobile ad hoc networks," in Proc. MILCOM, Oct. 17–20, 2005, vol. 2, pp. 1245–1251.

[8] M. Gerharz, C. de Waal, M. Frank, and P. Martini, "Link stability in mobile wireless ad hoc networks," in Proc. IEEE Conf. Local Comput. Netw., Nov. 6–8, 2002, pp. 30–39.

[9] M. Gerharz, C. de Waal, P. Martini, and P. James, "Strategies for finding stable paths in mobile wireless Ad Hoc networks," in Proc. IEEE Conf. Local Comput. Netw., Oct. 20–24, 2003, pp. 130–139.

[10] E. Y. Hua and Z. J. Haas, "Study of the effects of mobility on residual path lifetime in mobile ad hoc networks," in Proc. 2nd IEEE Upstate NY Workshop Commun. Netw., Nov. 18, 2005, pp. 33–37.

[11] E. Y. Hua and Z. J. Haas, "Path selection algorithms in homogeneous mobile ad hoc networks," in Proc. ACM Int. Wireless Commun. Mobile Comput. Conf., Jul. 3–6, 2006, pp. 275–280.

DOI 10.17148/IJARCCE.2016.5989