International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.11, November 2017 DOI:10.15693/ijaist/2017.v6i11.444-449

Review of Secure Routing and Energy Efficient in MANET using Hash Based Optimization

[1]Syed Azahad,[2] Shaik Hameeda
Research Scholar
Department of Computer Science
Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P., INDIA
e-mail: azahadsyed@gmail.com, hameeda999@gmail.com

Abstract: A mobile ad hoc network (MANET) is composed of multiple wireless mobile devices in which an infrastructure less network with dynamic topology is built based on wireless communication technologies. Novel applications such as location-based services and personal communication Apps used by mobile users with handheld wireless devices utilize MANET environments. This paper presents a Hash Based Optimization based routing algorithm that generates routes dynamically, following the concept of equal load distribution in the network. The local search component of HBO is modified using Simulated Annealing to provide an effective and energy efficient node selection mechanism. Experiments show that the algorithm exhibits effective load distributions and also provides dynamic random paths.

Keywords: HBO; Ad-hoc networks; Dynamic routing; Trust based routing, Security, Routing issues

1. INTRODUCTION

A MANET is a self-configuring network and self-preserving, which consists of wireless mobile devices with limited computing resources and bounded communication range. Dynamic topology, open medium, mutual collaboration, and lack of centralized management are the characteristics of MANET. Every mobile device in a MANET can move to any direction independently and establish communication channels with other mobile devices freely. When both mobile devices are in the wireless roaming range of the other node, they can establish communication directly; otherwise, a communication channel has to be built through multi-hop message routing within a MANET.In the recent times, trust based routing methods have also gained prominence. Trust is usually calculated by past experience and observed actions [17]. OSLR based routing scheme that uses trust levels of nodes during the selection process is presented in [16]. It presents a trust reasoning model that is based on fuzzy Petri net to evaluate these trust values. Other trust reasoning models that use OSLR are presented in [18, 19,20]. A cooperative routing strategy on the basis of trust and energy efficiency is presented in [23]. Dynamic trust and energy values are used to identify the nodes as selfish or altruistic. The traditional AODV algorithm is modified by incorporating trust and energy values. Effective routes eliminating selfish nodes were obtained. Emergent intelligence or group intelligence based routing mechanism is described in [21]. A logical clustering is created and the agents interact with each other. Inter and intra cluster communications are facilitated to collect details about the nodes in the network. Though this method is helpful, it relies on several static agents for appropriate working, hence are suitable only for specific type of networks. A method working exclusively on the basis of power consumption is presented in With cryptographic trapdoor function, only designated nodes, which have correct secret keys, can retrieve hidden information. However, two nodes need to exchange secret keys in advance before communicating with each other. Other approaches are based on cryptographic onion mechanism to prevent intermediate nodes from getting information within a message, such as the real identities of the source and destination nodes. With cryptographic onion approaches, nodes also have to consume heavily extra computation time to route messages in comparison with non-secure routing protocols. Geographic protocols in the third category have excellent benefits while all mobile devices must equip with GPS component. In order to provide an efficient anonymous secure routing protocol with communication anonymity for MANET environments, we introduce the Hash-based Optimization (HBO), whose design is based on collision-resistant one-way hash function and pseudo-name generation/exchange mechanism. Since no key cryptography or cryptographic onion mechanism is used in our protocol, HBO spends far more less computation time and network bandwidth during routing operations in comparison with existing solutions.In the recent times, trust based routing methods have also gained prominence. Trust is usually calculated by past experience and observed actions [17]. OSLR based routing scheme that uses trust levels of nodes during the selection process is presented in [16]. It presents a trust reasoning model that is based on fuzzy Petri net to evaluate these trust values. Other trust reasoning models that use OSLR are presented in [18,19,20]. A

cooperative routing strategy on the basis of trust and energy efficiency is presented in [23]. Dynamic trust and energy values are used to identify the nodes as selfish or altruistic. The traditional AODV algorithm is modified by incorporating trust and energy values. Effective routes eliminating selfish nodes were obtained

2. ROUTING PROTOCOLS IN MANETS

The three main types of MANET routing protocols are reactive, proactive and hybrid. [3]

1. **Proactive Protocols***:* Proactive protocols use table-driven routing. In this type of routing algorithms, every node in the list continuously maintains routing details of every other node. Changes in the network topology are updated by flooding the network periodically at short intervals. Therefore, there is a computation overhead for routing traffic but no delay for communication. Examples of proactive protocols are Destination Sequenced Distance Vector Routing (DSDV), Optimized Link State Routing Protocol (OLSR) etc.
2. **Reactive Protocols:** Reactive or on-demand protocols remove the computation overhead and instead use a route discovery process, whereby the network is flooded with RREQs every time a packet needs to be routed. Flooding uses bandwidth and there is also latency due to computation of the route for every packet. However, the overhead computation delay is removed. Examples of reactive protocols are Ad-Hoc On-Demand Distance Vector (AODV), Location Aided Routing (LAR), and Dynamic Source Routing (DSR) etc.
3. **Hybrid Protocols:** Hybrid protocols combine features from both proactive and reactive protocols. The high computational overhead of the table-driven system of proactive protocols and the delay due to route calculation in reactive protocols is usually reduced.

3. SECURITY ISSUES IN MANETS

Security issues in MANETs are due to its dynamic nature and low power, physical security etc. The following attacks are common in MANET [4]:

1. **Black hole attack**: It is also known as packet drop attack, a malicious node drops data it is supposed to forward, and hence reduces the packet delivery ratio. Depending on the compromised node, a black hole attack effectively can split the network in two components.
2. **Gray hole attack**: A gray hole attack is similar to black hole attack, however, it initially acts as a normal node, but after some time, starts dropping all or some packets it receives.
3. **Rushing attack**: Rushing attack is an exploit against on-demand protocols. It exploits the duplicate suppression mechanism in such protocols that are used to limit RR messages during transmission of data. Rushing attack forwards an RREP suppressing the valid RREP of another node and gain access to the communication between source and destination.
4. ***Worm hole attack***: Worm hole attack creates a link between two malicious nodes in the network. If the link becomes a part of the best path between the source and the destination, the malicious nodes are selected and they can monitor or disrupt communication in the network.
5. **Jellyfish attack**: In Jellyfish attack, packets are held for some time before they are propagated. Hence, a delay is added and end-to-end delay is adversely affected.

4. OVERVIEW OF SECURE ROUTING PROTOCOLS IN MANETS

Apart from the protocols mentioned in this section, authors have proposed several other trust based routing algorithms for MANETs. Marti et al. developed the Watchdog/Pathrater method as an optimization to the DSR protocol. [5] This protocol utilizes a Watchdog method to detect selfish nodes and a Pathrater method which find routes avoiding such nodes. The CONFIDANT protocol (Cooperation of Nodes, Fairness In Dynamic Ad hoc Networks) was a routing protocol that modified the Watchdog/Pathrater method by incorporating a trust scheme. [6][7] Depending on the Watchdog method, when a malicious node is detected, the information about the node is forwarded to all other nodes in the network by flooding an alarm message. This reduces their trust, and nodes are avoided if they have low trust values. CONFIDANT can detect selfish and malicious nodes but fails to prevent worm-hole attacks.

Another method based on DSR is ARIADNE [8] which uses the TESLA broadcast authentication protocol. While this method provides high security, using the TESLA protocol is unfeasible: due to the nature of

MANETs, precise time synchronization between neighboring nodes is unlikely. Moreover, this protocol fails to detect selfish nodes in the network.The ARAN protocol [9] detects malicious nodes in a network and uses asymmetric cryptography for authentication. This requires very high computation time and is unfeasible for low infrastructure systems of MANETs. The SEAD protocol [7] is based on DSDV and uses hash chaining for authenticating packets, while the SAR protocol extends AODV utilizes cryptography to select the most secure instead of the shortest path while routing. As with most cryptographic methods, it also suffers from high computation overhead and is generally unfeasible for MANETs.

5. HASH-BASED TRUST VALUES INTO ROUTING PROTOCOL

In this section, we present the detailed design of HTVR Protocol. HTVR Protocol contains the following phases along with corresponding control packets or data packet: Route Request phase, Route Reply phase, Data Transmission phase, and Route Maintenance phase.The routing operations of HTVR Protocol is similar to AODV [14]. All nodes do not need to exchange any routing table information before communicating with another node. The broadcast mechanism is adopted to build the routing table dynamically in each node. Each node maintains just few useful records in its routing table when performing routing discovery. In a routing table, the out-of-date records will be superseded by the up-to-date ones.

Our assumptions are described as follows:

- Each node has a unique ID which is only known by itself at default.
- All nodes can detect route failures.
- All nodes are willing to forward packets according to HTVR protocol.
- All nodes have implemented the same collision-resistant one-way hash function.
- All adversaries have unbounded eavesdropping capability but bounded computing resources.

A. Route Request phase

In this phase, each Ni receives a RREQ packet with the following format:

[*RREQ*, r_{ii1}, *seq*, *H*(*seq*, ID_D)]

Before sending a RREQ packet, *S* generates r_0 by calculating *H*(ID_S , *t*). Utilizing the real identity and timestamp can produce the unique pseudonym, since the identity given by S is unique and is only known by itself. Then, *S* calculates and stores *H*(r_0, *seq*) for later using after generating r_0.

When N_i receives the RREQ packet, first, it puts the *seq* and its ID_i to *H*, and compares with *H* (*seq*, ID_D) given by previous hop. If they match, it means that the node is *D*. Because of the feature of unique *ID*, only *D* can match *H*(*seq*, ID_D) successfully. If matching fails, N_i records the seq and r_{ii1} into his routing table for later using. Second, it generates r_i according to equation (1):

$$r_i = r_{ii1} \oplus H(ID_i) \qquad (1)$$

Using $H(ID_i)$ can ensure that r_i is unique absolutely, since each node has a unique ID. After N_i generates r_i, it replaces r_{ii1} to r_i, computes and records $H(r_{ii1}, seq)$ for later using. Finally N_i broadcasts the modified packet locally. Each N_i will do the same action as above until this RREQ packet is received by *D*. At the end of the RREQ phase, each N_i has established shared secret with the previous and next hops.

B. Route Reply phase

In this phase, each N_i receives a RREP packet with the following format:

[*RREP*, *H*(r_i, *seq*), *H*(ID_D , *H*(*seq*, ID_D))]

After receiving the RREQ packet sent from *S*, *D* will initiate the RREP packet. It generates *H*(r_i, *seq*) with r_{ii1} and *seq*, and puts ID_D and *H*(*seq*, ID_D) to *H* to produce the message authentication code (MAC) which is used to verify itself. Since only *D* knows ID_D , it is impossible to be forged. At first, as each N_i receives the RREP packet, it verifies the packet whether it is legal or not by comparing each record with *H* (r_i, *seq*) which it stores in the RREQ phase. The RREP packet is sent from the node which participates the RREQ phase if verifying successfully. Otherwise, it discards this packet. Second, it generates the *H*(r_{ii1}, *seq*) and replaces *H*(r_i, *seq*). Afterwards, it broadcasts the modified packet locally. Each N_i does the same process as above until the RREP packet arrives S. At the end of the RREP phase, the routing path is established and verified completely.

C. Data Transmission phase

After routing discovery finishes, the routing path is established completely as well. Only N_i which participates previous phases will forward DATA packets. Every N_i receives a DATA packet with the following format:

[*DATA*, *n*, *H*(*n*, r_{ii1}), *data*]

As *S* starts to transmit data, it chooses a random number *n* and generate *H*(*n*, r_{ii1}) by putting r_0 that is produced in the RREQ phase with n. This phase is similar to the RREP phase. Each N_i verifies the validity of each DATA packet sent from previous hop by calculating *H*(*n*, r_{ii1}). If N_i which does not join the routing discovery cannot verify the DATA packet, it throws the packet away. Next, N_i uses equation (1) to compute r_i after the packet passes the verification, generating a new *H*(*n*, r_i) by using the increased n and r_i. Besides, N_i will protect the data by using an efficient method before forwarding this packet. Finally, it

broadcasts the modified packet locally. Such processes continue until *D* gets the DATA packet.

D. Route Maintenance phase

As we assume before, nodes can detect route failures by checking re-transmission count. If the count exceeds a specific threshold, the node looks up the routing table to find the corresponding record that shares with previous neighbors, and generates a RERR packet with the following format:

[*RERR*, $H(r_i, seq)$]

The node which receives this packet will validate the validity of this packet by checking $H(r_{ii1}, seq)$. It ignores the packet as the packet is checked unsuccessfully. Otherwise, it deletes the corresponding record directly.

E. Routing table maintenance

As we mention above, the operation of HTVR is similar to AODV [14]. We only carry little information when operation of our protocol. Each node needs to keep at most five fields, and the form of routing table is shown below:

Obviously, for all nodes, the ID_D field is empty except *S*, since only *S* knows ID_D . All N_i do not need to record r_i, since they can retrieve it by using equation (1). However, this may be a tradeoff between saving computation and space resources. Only nodes which forward the RREQ packet except *D* will calculate and store $H(r_{ii1}, seq)$ for verifying the validity of RREP packet later. Besides, nodes can delete the entire record when successfully validating the RERR packet. If being out -of-date, this record also can be deleted by comparing its corresponding timestamp with current time. Based on this table maintenance mechanism, our scheme can save storage space and improve efficiency of record search.

A. SECURITY ANALYSES

In this section, we do an anonymity analysis about how we promise the privacy in the proposed protocol, and then, four major attacks we can defense are discussed in security analysis. For giving a strict examination, our analyses are based on the hostile environment where adversaries can overhear packets with infinite ranges but finite computing resources.

A. Anonymity analysis

We will look into the anonymous properties including the identity anonymity, location anonymity, and route anonymity in this section.

1) Identity anonymity

In HTVR, only ID_D is involved in RREQ and RREP packets. The format of RREQ and RREP packets are:

$$[RREQ, r_{ii1}, seq, H(seq, ID_D)]$$

$$[RREP, H(r_i, seq), H(ID_D, H(seq, ID_D))]$$

We observe the format: the ID_D is encrypted with a *seq* by *H*, and the *seq* is different in each session. Due to the characteristic of a collision-resistant one-way hash function, different parameters will gain different outputs. Thus, it is
Difficult for adversaries to infer ID_D. This makes HTVR provide identity anonymity in MANETs.

2) Location anonymity

Some anonymous secure routing protocols, like MASR and AnonDSR [18], take advantage of the padding method to thwart that adversaries deduce the distance from source to destination nodes by comparing the length of those packets. In HTVR, it adopts another way to achieve the same effect without using padding method. All nodes communicate with others by using different pseudonym in each session, and each node only knows the pseudonym of previous and next hops. Due to this feature, if the distance from a node to another node is more than one hop, they cannot find any information about the location of each other. Therefore, HTVR can provide location anonymity in MANETs.

3) Route anonymity

In general, adversaries collect information by eavesdropping, analyze all packets and try to find some useful information (for example, the same sequence numbers or regular rules of packet size) to infer the traffic pattern. This attack is called traffic analysis. In HTVR, even if the adversaries can collect all packets during the RREQ, RREP, or DATA phases, they still cannot get any useful information by analyzing. The reasons are discussed as following: In the RREQ phase, the *seq* is different in each session. The ID_D and *seq*, which are encrypted by collision-resistant one -way hash function, will be different in each session as well. In the RREP and DATA phases, the $H(r_i, seq)$ and $H(n, r_{ii1})$ are different in each hop, respectively. For above discussion, adversaries are incapable of finding out the relation among RREQ, RREP, or
DATA packets. Hence, HTVR can provide route anonymity in MANETs.

B. Security analysis

In terms of previous researches, four main attacks named replay attack, spoofing attack, route maintenance attack, and DoS attack are launched frequently. Consequently, we show how we guard against them carefully in this section.

1) Replay attack

For replay attack, adversaries resend the same packets eavesdropped by themselves at previous communication sessions. If adversaries resend the RREQ packet to the node which receives the same RREQ packet early, the node throws this RREQ packet away since the *seq* repeats. However, adversaries may

resend RREP, DATA, or RERR packets to launch attack. A RREP packet is verified one time for a node in a session. Hence, if receiving the same RREP packet, the node throws this RREP packet away. In HTVR, the field *n* increases hop-by-hop in the DATA packet. Thus, the node throws the DATA packet away when receiving the DATA packet that is involved in the same value of field *n*. When receiving the same RERR packet, the node discards this packet since the corresponding records are deleted already, and it cannot verify this RERR packet anyway.

2) Spoofing attack

It is impossible for adversaries to launch spoofing attack, since the identity anonymity is guaranteed in HTVR.

Adversaries cannot disguise any node to attack other nodes, because they do not know the real identity of any one.

3) Route maintenance attack

In general, adversaries send fake RERR packets to deceive the source node to select another routing path or execute routing discovery again. In HTVR, no new incoming adversaries can send fake RERR packets, b ecause they do not have any secret information shared with any nodes.

4) DoS attack

The DoS attack means that multiple adv ersaries cooperate to deplete the resources of the target. In order to launch this attack, adversaries need to identify the target. In HTVR, it is impossible for adversaries to identify a node by analyzing route control packets or data packets, because the identity anonymity is guaranteed.

6. CONCLUSIONS

Trust based algorithms attempt to increase the security of communication in MANETs by introducing an authentication scheme. A fundamental issue of any trust based algorithm is the definition of trust. Different authors propose different methods to calculate trust in literature; however, these parameters tend to be specific for certain types of configurations and not generic, therefore QoS improvement varies depending on the specific network.

Different papers consider different parameters for analysis of performance, however, they can suffer in some parameters not consider. For instance, protocols like FrAODV increase communication delay due to the route calculation algorithm. Protocols like TARP only consider parameters like power and encryption and do not consider packet forward ratio or end to end delay. Algorithms based on proactive protocols also contain the innate computational overhead issue of all proactive methods. Parameters that can be considered for comparing or designing trust based routing algorithms include end-to-end delay, packet forward ratio, computation overhead, latency, infrastructure etc. apart from security issues, specifically various types of DoS attacks. [5][20]

This survey highlights that there are possible ways of improving secure routing in MANETs. Evidently, no current method offers improved QoS in all parameters and security from all possible attacks at the same time. New protocols need to consider both QoS metrics as well as security issues. Gray hole attacks are difficult to resolve for most trust based protocols since the compromised node can build up high trust value before it starts dropping packets. If a malicious node performs activities not covered by the trust parameter (for instance, if a trust calculation method considers packet transfer rate and the malicious node does not drop packets), trust based methods can be vulnerable to the attack. Similarly, several protocols (including cryptographic protocols) cannot easily prevent worm-hole attacks. Therefore, protocols should consider a collection of parameters to calculate trust, depending on the specific properties of the network. Another vital issue in a MANET is power consumption. In [22], [23], authors consider energy efficiency as a parameter and have improved previously existing trust based algorithms. Likewise, highly secure algorithms can be modified in the future to add a parameter corresponding to power which will make them energy efficient as well as secure and hence safe and feasible. However, this should not be done at the expense of deterioration in QoS of the network.

REFERENCES

1. L. Bao, “A New Approach to Anonymous Multicast Routing in Ad Hoc Networks,” Proceedings of the International Conference Communications Networks, pp. 1004- 1008, China, 2008.
2. Castelluccia and P. Mutaf, “Hash-Based Dynamic Source Routing,” Lecture Notes in Computer Science, vol. 3042, pp. 1012-1023, 2004.
3. http://www.cryptopp.com/benchmarks.html, March, 2010.
4. S. Dabideen, B. R. Smith and J. J. Garcia-Luna-Aceves, “An End-to-End Solution for Secure and Survivable Routing in MANETs,” Proceedings of the 2009 7th International Workshop on the Design of Reliable Communication Networks, pp. 183-190, Alexandria, VA, United States, October, 2009.

5. S. Denh, C. Rex and B. Lichun, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks," Proceedings of the 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 267-276, Vancouver, BC, Canada, October, 2006.
6. El-Khatib, L. Korba, R. Song, and G. Yee, "Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks," Proceedings of the International Confer- ence on Parallel Processing Workshops, pp. 359-366, Kaohsiung, Taiwan, October, 2003.
7. D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Proceedings of the ACM Special Interest Group on Data Communication - Computer Communication, Palo Alto, 1996.
8. J.-C. Kao and R. Marculescu, "Energy-Efcient Anonymous Multicast in Mobile Ad-Hoc Networks," Proceedings of the International Conference on Parallel and Distributed Systems, Hsinchu, Taiwan, December, 2007.
9. Karp and H.T. Kung, "GPSR: Greedy Perimeters Stateless Routing for Wireless Network," Proceedings of the Annual International Conference on Mobile Computing and Networking, pp. 243-254, 2000.
10. Kong and X. Hong, "ANODR: Anonymous On Demand Routing with Untrace- able Routes for Mobile Ad-hoc Networks," Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 291-302, 2003.
11. Liu, F. Fu, J. Xiao, and Y. Lu, "Secure Routing for Mobile Ad hoc Networks," Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 314-318, Qingdao, China, 2007.
12. Pan and J. Li, "MASR: An Efcient Strong Anonymous Routing Protocol For Mo-bile Ad Hoc Networks," Proceedings of the International Conference on Management and Service Science, Wuhan, China, September, 2009.
13. S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," Proceedings of the International Conference on Advanced Information Networking and Applications, Vienna, Austria, April, 2006.
14. X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Transactions on Parallel and Distributed Systems, vol. 19, pp. 1297-1309, 2008.
15. X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Rout- ing Protocol," IEEE Transactions on Mobile Computing, vol. 4, pp. 335-348, 2005.
16. Yu, M. Zhou and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," IEEE Transactions on Vehicular Technology, vol. 58, pp. 449-460, 2009.
17. Zhao and H. Shen, "A Low-cost Anonymous Routing Protocol in MANETs," Proceedings of the International Conference on Computer Communications and Networks, San Francisco, CA, United States, August, 2009.
18. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H.Deng, "Anonymous Secure Routing in Mobile Ad-hoc Networks," Proceedings of the 29th IEEE International Conference on Local Computer Networks, 102-108, Tampa, FL, United States, November, 2004.