Different Secured Routing Protocols for Mobile Ad Hoc Networks and its Vulnerabilities: A Review

Arnab Majumdar
Department of Metallurgical and Materials Engineering
National Institute of Technology, Durgapur
West Bengal, India
xie.7802@gmail.com

Saptarshi Banerjee
Assistant Software Engineer
Tata Consultancy Service
West Bengal, India
banerjee.saptarshi44@gmail.com

***Abstract*—A Mobile Ad Hoc Network (MANET) is self-organizing, infrastructureless, multi-hop network. The open and distributive nature of MANET posses a big challenge to design the secure routing protocols. So, secure routing in MANET has become the important research area. Taking into consideration that there is the possibility for the proper authenticated nodes to come under the control of malicious agents, there must be the presence of secure routing protocols which will permit nodes to work in unfavorable potential system within MANET. In this paper we have illustrated different existing secured routing protocols with their advantages and disadvantages. We have also described the necessity of robust and light weight secured routing protocols to solve problems of existing secured routing protocols.**

Keywords—Mobile Ad Hoc network; security threats; fidelity; malicious nodes; routing path; wormhole

I. INTRODUCTION

In Mobile Ad Hoc network, routing protocols are designed keeping the idea of efficiency and performance of the network [1]. Ad Hoc networks are the self-configuring structures which have no fixed infrastructure and hereby nodes connecting the network are depended on each other.

For both wired and wireless networks, there is high demand for security. Other than wired connection, there comes a no of problems regarding the degree of security in the wireless structure [2]. It is because of its dynamic topology, open nature etc. This weakness of network has becomes the main focus of attacks of malicious agents [3]. So, in this network system, security is the most important issue for its existence. Here in the network layer, we have to give focus to possible ways of attack which can take place in the system. There must be provided with a multilayered security system rather than single layer security for the network. Some of the threats towards network system are Black hole attack, Gray hole attack, Wormhole attack, Jellyfish attack etc.

In the presence of these threats, the sensitive information should not be sent as the details and privacy gets lost or can be hacked in presence of malicious nodes, thus there is no reliability on individual single path. To get out of this threat, we must send the multiple copies of same information through multiple disjoint paths where there is the possibility of leakage of information. Similar to this wireless network, internet service gets affected by malicious agents mostly in the business network, where there comes storage of data, official details which can be lost due to invasion [4]. Ad Hoc network is composed of independent nodes which communicates through multi-hop radio network and thus makes a decentralized connection with all the nodes in network. The node connection changes from time to time with the arrival and departure of nodes, resulting in dynamic nature of the network topology.

Again the malicious nodes are not secured enough, causing disrupt in the route discovery phase. Due to the open nature of Ad Hoc network system, they can be easily accessible in the insecure environment and are more prone to attack caused by the malicious nodes in different network systems. From the research, it is known that the misbehaving nodes cause damage to service system in the MANET. Thus, the routing protocols being binding forces in the network becomes the common target of these malicious nodes. The goal of this paper is to study various secured routing protocols in MANET and to illustrate their merits and demerits.

This paper is organized as follows:

In this paper, Section II presents different secured routing protocols with its vulnerability. Again, this section is sub-divided into (A) Trust Oriented Secured Routing Protocols, (B) Incentive Oriented Secured Routing Protocols and (C) Detection and Isolation Oriented Secured Routing Protocols. Finally Section III presents the conclusion of the paper with Section IV containing Acknowledgment.

II. DIFFERENT EXISTING SECURED ROUTING PROTOCOLS

The MANET secure routing schemes, which are traditionally used to prevent the mischief activities of malicious nodes, use three approaches:

A. Trust Oriented Secured Routing Protocols

B. Incentive Oriented Secured Routing Protocols

C. Detection and Isolation Oriented Secured Routing Protocols

978-1-4799-6908-1/15/$31.00 ©2015 IEEE

Now, we are hereby to review the different types of routing protocols with their advantages & disadvantages.

A. TRUST ORIENTED SECURED ROUTING PROTOCOLS

Yi *et al* have proposed security aware Ad Hoc routing also termed as SAR [5]. In his proposition, SAR has classified the nodes on basis of their trust values. On the basis of this classification, the similar nodes with same trust level share a secret group key. In determining route, the source node agrees to have minimum number of security requirements, which a node generally requires in order to complete its routing path from source to destination. Source node can also agree to make path by encryption of route request packets with certain specified keys for specific levels. In it keys become the main defect for the scheme, which can create problems when malicious nodes will control the keys inspite of having high security while controlling the secret group keys.

Nekkauti and **Lee** have given birth to a certain trust based adaptive routing protocol [6]. This protocol uses the mechanism of conversion of the codes into order while covering the route path between the source and destination through all other nodes. This scheme supports greater degree of individualism of nodes to operate in routing path but the greatest disadvantage is it can't protect network system from malicious activities where there is the selective dropping and modification of packets which are agreed to be forwarded, under malicious nodes.

Lee and **Singhal** have stated the secured routing protocol [7] which operates using pre-observed behavioral pattern along with reference to other nodes nearby the operating one and thus gives the quantitative value of trust to operating nodes in MANET. This protocol gives the basis of anonymity but is not at all protected from the malicious nodes which can grasp well behaving nodes in order to drop trust messages, thus makes the protocol ineffective.

Mangrulkar and **Atique** have proposed the scheme [8] in which the routing will add an extra field to store the trust value levels of node. This shows how much a node can be trusted by neighboring. Considering all trust values of nodes, information of the router will be transmitted through nodes which have highest level of trust value. The utility of this scheme lies in the fact that it saves the power of unwanted transmission of information through the nodes having low trust value, also saves the band width which is very important in MANET system. Here the trusted path will be used irrespective of range of distances, which can be safely used in communication purpose of network. The trust value can be calculated depending upon complete reply path that can be need by source node for further communication.

Yan, **Zhang** and **Virtanen** have developed a model which gives trust values to nodes depending upon observation of node's behavior [9]. Application of this trust evolution is similar to that of SAR [5] where other than it, Yan fails to suggest a way so that source node will stop the node to carry forward the details inspite of having low trust value, making it a part of routing path from source to destination.

Saha *et al* have proposed another scheme "FBOD" (Fidelity Index Based On-Demand Secure Routing) for routing in mobile Ad Hoc network [10] which totally varies from other existing routing protocols. Here packets routed on the basis of specific criteria of nodes known as "fidelity". Through this scheme the complex computation in transmission of data gets lowered a lot. This scheme shows the network activity for routing purpose of packets gets decreased for each of the nodes. This scheme also stops the attacks of malicious nodes in MANET.

Boukerche *et al* have proposed a protocol "SADAR: Secure Distributed Anonymous Routing Protocol" [11]. The main function of the above stated protocol is to permit nodes to take part in the routing system without granting their individual participation in routing system. The author suggests that this protocol will able to stop malicious activities of dropping down of packets by operating within system interface through promiscuous mode and will detect discrepancies regarding the unnatural packet transmission through nodes. This protocol operates same as that of **Marti *et al*** [12] "Watchdog" operation.

Pirzada and **McDonald** also have given a model which shows trust based communication in Ad Hoc network [13]. This model depends upon the facts such as:

a) Passive and Active recognition of packets.

b) Recommendation from other nodes regarding possible short route replies.

c) Information regarding routing errors.

This scheme is also threatened by the malicious nodes present here who can discharge the packets selectively and will accuse nodes which are working with no discrepancies.

Davis *et al* have proposed secured on demand routing scheme in MANET known as Robust source Routing (RSR) [14] in which protocols has the capacity to mitigate against the high profile malicious nodes, in addition to providing data, authenticity and integrity checking of network. RSR prevents the selfish activities where it stops the selective dropping of packets which are agreed to be put forward by nodes. Also with study, it is known that RSR possess capacity to maintain high delivery even when almost all nodes in MANET become malicious in nature.

B. INCENTIVE ORIENTED SECURED ROUTING PROTOCOLS

Zhong, **Chen** and **Yang** have presented a new scheme "SPRITE", which is simple working, credit based and cheat proof system in MANET [15]. In MANET nodes, this protocol provides the initiative to co-operate and to collect actions

honestly. The utility of this protocol is that it doesn't go for all tamper resistant modules rather supports to have on-line access to the central system called Credit Clearance Service (CCS). This CCS considers the charge of sending message through nodes. But the basis of this scheme depends on the assumption that there is the availability of on-line access to a CCS, which doesn't go for real Ad Hoc networks and can't able to confirm on-line entity access directly.

Buttyan and **Hubaux** have suggested the scheme where the protocol incentive towards stimulating co-operation in the MANET [16]. In this scheme, the network nodes must have hardware module which is resistant towards tampering. This scheme never allows the selfish activities of nodes operating in this structure. But this scheme fails to achieve the wide spread usage due to requirement of the hardware which is tamper resistant.

C. DETECTION AND ISOLATION ORIENTED SECURED ROUTING PROTOCOLS

Marti *et al* [12] have proposed a scheme in which they stated that those MANET nodes will be mitigated which fails to forward the packets through nodes. In order to identify misbehaving nodes, scheme uses "Watchdog" and to avoid them, protocol uses "Pathrater". Watchdog is an essential operation in MANET which guides node is work in promiscuous mode. It is based on assumption that when packet is moving from one node to other, then there should have transmission between them. While transmission is going on, neighboring node should hear transmission which is carried out by operating nodes, and if it fails to do so, then if will likely, be called as malicious node having low rating. This scheme thus shows several weaknesses. So, author stated that the main weakness of "Watchdog" operation is that it fails to recognize the misbehaving nodes within the network when they are under the presence of ambiguous collision, collusion, collision of receiver, limited power of transmitter and partial dropping.

Buchegger and **Le Boudec** have presented a new type of protocol called "CONFIDANT" [17] (Co-Operation of Nodes: Fairness in Dynamic Ad Hoc Network). This protocol is used for the detection and isolation of misbehaving nodes, where "CONFIDANT" carries out work by reputation system [18] where the trust and routing values are calculated by experience, observation and behavior of other nodes, present in network. Here the nodes by judgment blacklisted those which are found to be misbehaving and hence gets isolated within the system. The main drawback is that the reputation system associated with this protocol fails to give any protection against false accusation and thus protocol is influenced towards blackmailing. The merit of this scheme is that it can detect selfish nodes, wormhole nodes and isolate them from system which causes dropping of packets.

Nagrath and **Gupta** have presented a scheme [19] where they stated that nodes operating in MANET are sometimes threatened by the attackers to get into system and will carry out the attacks by stealing and altering information, a type of which is known as "Wormhole Attack". In this attack, the existing nodes are not disturbed and malicious agents interfere in route development process. Wormhole attacks damage the routing path in AODV, DSR and OLSR. This attack can damage the entire MANET system by its two modes of attack, hidden mode and participation mode, where attackers damage network system totally. This attack can be prevented by using extra hardware, which though increases cost protects network. Also, to reduce cost, there can be the use of algorithm, showing good performance using low overhead.

Choi *et al* [20] have presented a protocol, "WAP: Wormhole Attack Prevention" which detects fake routes. It also prevents wormhole nodes to appear in route discovery phase which can be achieved utilizing the method of neighbor node monitoring of each node. The mechanism of this protocol came from the basis lead by DSR protocol. The main advantage is that WAP can prevent the wormhole invasion in networking system with no utilization of any extra hardware. But the protocol gets restricted from its work when there occurs the attack of other foreign malicious nodes and they have their high overheads. Also this secure routing protocol does not address energy constraints of node for routing.

Awerbuch *et al* have presented routing security protocol [21] which has its main focus to withstand the byzantine failure of MANET nodes, working individually in system. In this scheme, the nodes used to maintain a weight list of them considering the track of their performances within network, on the basis of which it becomes easier in route discovery phase to avoid path containing faulty nodes. After detecting the faults in the established path, adaptive probing techniques is used to capture the faulty links, hence gets low rating and are avoided in the system. Through these probing technique, we can able to identity the faulty zones in the network which results due to non-malicious agents. But main barrier of this protocol is that they are ineffective in presence of malicious agents only because nodes can able to recognize the probing packets from others. Thus an opponent node will behave good and well when it is probed state and otherwise it will show malicious activities in the node intervals. This scheme doesn't address energy constraints.

Patwardhan and **Iorga** [22] have proposed the secured routing protocol model called SecAODV, which is modified form of AODV, where all the nodes are provided with a certain IPv6 address value within the MANET. In this scheme, the secured communication channel is established in between source and destination node depending upon the idea of Statistically Unique and Cryptographically Verifiable (SUCV) who confirms secured and secret binding between IPv6 address and key node. [23] In this scheme, there is no requirement of trust certificate (CA). Still this protocol is restricted in working zone since here it is necessary for all the MANET nodes to contain a certain IPv6 address. It fails to stop or prevent the selective dropping of packets, as the probing packets can be easily recognized from others. Along with this, scheme does not have address for energy constrains.

Saha *et al* [24] have proposed semi centralized multi authenticated RSSI based solution to Sybil attack. It provides a hybrid solution where the entire network is subdivided into small subgroups under the supervision of each node, acting as the central authority. Here each of the subgroups has RSSI detector nodes. The advantage is that even when false reading is sent, the problem will be restricted in the group only and this false detail will not affect the entire network. The demerit is that if any of detectors in the group can be compromised then there will be trouble, also the scheme does not address any energy constraints and can't tackle other attacks other than Sybil.

Just *et al* [25] and **Kargl *et al*** [26] also have come up with a scheme where there is mechanism of identifying the selfish and malicious nodes in Ad Hoc network system. This protocol goes through probing mechanism as stated by **Awerbuch *et al*** [21] where they can be recognized from others. The problem regarding this protocol is that the end to end delay is high, and does not address energy constraints.

Saha *et al* [27] have proposed Priority Based Protocol which has capacity to detect malicious nodes with no notification to central authority. Here the nodes will maintain priority list of neighbors and when the value will go below the threshold level, the node will be disconnected from the system. Nodes here can also upgrade themselves and act as per node, as they are independent of trust certificate (CA). Also if any of the nodes are found showing their malicious activities within the network, then their importance level will be decreased. The merit is that this protocol can able to detect different attacks like Black hole attack, Gray hole attack, but fails to combat Jellyfish. This scheme can be used in distributed manner which provides less network dependence of nodes.

III. CONCLUSION

From the above discussions, it is clear that existing secure routing protocols are not sufficient to eliminate the malicious nodes which causes the dropping or modification of packets in the network and as a result, there causes severe communication problems in MANET. Most of the protocols are more specifically focused on mitigating certain attacks, while others show a drop in performance, pertaining to packet delivery fraction, normalized routing load and end to end delay. Besides we have seen that some of the protocols fail to judge the energy consumption of the nodes present in trustworthy route, which is also an important issue in MANET. Analysis shows that making a protocol more secured; we have to make other QoS parameters compromised, implying a requirement of trade off. In the above work, we have classified the secured routing protocols in different parts with specific cause and reasons.

Firstly, Trust Oriented Secured Routing Scheme is reliable and trustworthy but is obtained at the loss of quantity of service of the systems.

Secondly, Incentive Oriented Secured Routing Scheme tries to decrease the attacks on the network through hardware and incentives but can't able to eliminate them totally, also there is no improvement in QoS.

Finally, Detection and Isolation Oriented Secured Routing Scheme effectively mitigate the attacks of malicious nodes, but done at the cost of QoS of the system. Also they are attack specific to malicious nodes and are not able to detect the other attacks.

From these studies, it has been observed that there is the necessity of much more secured routing protocols for MANET which will be energy efficient, and have the capacity to mitigate all malicious attacks considering all other QoS parameters that are required for the network.

IV. ACKNOWLEDGEMENT

Sincere thanks to Prof. Himadri Nath Saha for providing inputs and useful comments and suggestions in order to improve the quality of this paper. Also thanks to anonymous reviewers who gave many valuable details and inputs to enrich this paper.

REFERENCES

[1] P Narayan, and V.R. Syrotiuk, "Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool," *in Proc. of Second International Conference, ADHOC-NOW*, Springer, Montreal, Canada, October 2003, pp. 25-36.

[2] Hong Mei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, Vol. 40 ,Issue: 10, pp. 70 -75, October 2002.

[3] Y.Xiao, X. Shen, and D.Z. Du (Eds), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless/Mobile Network Security*, Springer, Chapter 12, pp. 1-38, 2006.

[4] G. Theodorakopoulos and J.S. Baras, "Trust Evaluation in Ad Hoc Networks," *in Proc. of ACM Workshop on Wireless security (WISE'04),* October 2004, pp.1-10.

[5] S. Yi, P. Naldurg and R. Kravets, "Integrating Quality of Protection into Ad Hoc Routing Protocols*," in Proc. of the 6th World Multi Conference on Systematic, Cybernetics and Informatics (SCI 2002)*, August 2002, pp. 286-292.

[6] R.K Nekkanti and C.W Lee, "Trust Based Adaptive on Demand Ad Hoc Routing Protocol," *in Proc. of the 42nd Annual Southeast Regional Conference*, April 2004, pp. 88-93.

[7] H. Li and M. Singhal, "A Secure Routing Protocol for Wireless Ad Hoc Networks," *in Proc. of the 39th Hawaii Informational conference on Systems Science (HICSS-39)*, January 2006, pp. 225-234.

[8] R.S. Mangrulkar, and Dr. Mohammad Atique "Trust Based Secured Ad Hoc on Demand Distance Vector Routing Protocol for Mobile Ad Hoc Network*," in Proc. of Sixth International Conference on Wireless Communication and Sensor Networks (WCSN)*, December 2010, pp. 1-4.

[9] Z. Yan, P. Zhang and T. Virtanen, "Trust Evaluation Based Security Solution in Ad Hoc Networks," *in Proc. of the 7th Nordic Workshop on Secure IT Systems (NORDSEC 2003)*, October 2003.

[10] Himadri Nath Saha, Debika Bhattacharyya and P. K. Banerjee, "Fidelity Index Based On Demand (FIBOD) Secure Routing In Mobile Ad hoc Network," *in Proc. of International Conference on Parallel Distributed Computing Technologies and Applications (PDCTA),* Springer, vol.203, part-II, September 2011, pp.615-627.

[11] A. Boukerche, K. El-Khatib, L. Xu and L. Korba "An Efficient Secure Distributed Anonymous Routing Protocol for Mobile and Wireless Ad Hoc Networks," *Computer Communications, Elsevier*, Vol. 28, Issue 10, pp.1193-1203, July 2004.

[12] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigation Routing Misbehavior in Mobile Ad Hoc Networks," *in Proc. of 6th annual international conference on Mobile Computing and Networking*, August 2000, pp. 255-265.

[13] A.A. Pirzada, C. McDonald, "Establishing Trust in Pure Ad Hoc Networks," *in Proc. of the 27th Conference on Australasian Computer Science (CRPIT'04),* January 2004, pp. 47-57.

[14] Clude, R. Davis, Maheswaran, "A Secure MANET Routing Protocol with Resilience Against Byzantine Behaviors of Malicious or Selfish Nodes," *in Proc. of 21st International Conference on Advanced Information Networking and Application Workshop*, May 2007, pp. 19-26.

[15] S. Zhong, J. Chen, Y. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Networks," *in Proc. of IEEE INFOCOM*, Volume 3, March 2003, pp. 1987-1997.

[16] L. Buttyan and J.P. Hubaux, "Stimulating Co-Operation in Self-Organizing Mobile Ad Hoc Networks," *ACM Kluwer Mobile Networks and Applications*, Vol. 8 Issue 5, pp.579-592, October 2003.

[17] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDENT Protocol," *in Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02),* June, 2002, pp. 226-236.

[18] P. Resnick, K. Kuwabara, R. Zeckhauser and E. Friedman, "Reputation Systems," *Communications, ACM.* Vol. 43, Issue 12 pp. 45-48, December 2000.

[19] Preeti Nagrath and Bhawna Gupta, "Wormhole Attacks in Wireless Ad Hoc Networks and their Counter Measurements: A Survey," *in Proc. of 3rd International Conference on Electronics Computer Technology (ICECT)*, IEEE, April 2011, pp. 245-250.

[20] S. Choi, D. Y. Kim, D. Y. Lee, and J. I. Jung "WAP: Attack Prevention Algorithm Mobile Ad Hoc Network," *in Proc. of IEEE International Conference on Sensor Network, Ubiquitous and Trustworthy Computing*, June 2008, pp. 343-348.

[21] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *in Proc. of the ACM workshop on wireless security (WiSE'02),* September, 2002, pp. 21-30.

[22] A. Patwardhan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks," *in Proc. of the 3rd IEEE – International conference on Pervasive Computing and Communications,* March, 2005, pp. 191-199.

[23] T.S Messerges, J. Cukier, T. A. M. Kevenaar, L.Puhl, R. Struik and E. Callaway, "A Security Design for a Personal Purpose Self-Organizing Multihop Ad Hoc wireless network," *in Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 1-11, October 2003.

[24] Himadri Nath Saha, Debika Bhattacharyya, P. K. Banerjee, "Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack," *International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004),* Vol. I, Issue 4, pp. 338-341, December 2010.

[25] M. Just, E. Kranakis and T. Wan, "Resisting Malicious Packer Dropping in Wireless Ad Hoc Networks," *in Proc. of ADHOCNOW'03*, October 2003, pp. 151-163.

[26] F. Kargl, A. Klenk, S. Schlott and M. Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks," *in Proc. of the 1st European Workshop on Security in Ad Hoc and Sensor Networks (ESAS 2004)*, August 2004, pp. 152-165.

[27] Himadri Nath Saha, Debika Bhattacharyya, P. K. Banerjee, "A Priority Based Protocol for Mitigating Different Attacks in Mobile Ad hoc Networks," *International Journal of Computer Science & Communication*, Vol. 1, Issue: 2, pp. 299-302, December 2010.