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. 4, Issue 10, October 2016

Grade Trust Using Routing Protocol in Mobile Ad Hoc Networks

P.Bharathi[1], R.Marutha Veni [2]

Department of Computer Science, Dr. SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India[1]

Department of Computer Science, Dr. SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Trust-based secure routing in MANETs has attracted lot of research attention worldwide. It is effective in providing secure routing by isolating malicious nodes and other overheads from MANETs. This paper proposes, Grade Trust, a secure routing protocol for MANETs based on the trust levels of network nodes. It uses trust to isolate black hole routing attacks thus offering secure routing of data traffic as well as improved packet delivery ratio. Preliminary simulation results have shown that trust compromise and packet delivery ratio is better in Grade Trust compared to traditional routing protocols, such as AODV and FSR.

KEYWORDS*:* Secure Trust Based Routing: Background Study, .Gradetrust: A Secure Routing Protocol (Functioning, Routing) Performance Analysis, Packet Delivery Ratio , End-To-End Delay , Trust Compromise

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of mobile devices (called nodes) that communicate with each other without the use of infrastructure such as access points or base stations. These self-configuring networks are capable of self-directed operations and can be deployed easily. They are also referred to as Self-Organizing Networks (SON), in which the nodes cooperate among themselves to provide connectivity and operate without centralized administration [1]. MANETs are used in a variety of applications, such as, vehicular ad hoc networks (VANET), sensor networks, military networks, robotic mobile networks, etc.

For the effective functioning of MANETs, routing protocols are needed for the nodes in the network to communicate and create appropriate paths for data transmission. These logically structured paths enable the transfer of data packets to a destination node travelling through multiple intermediate hops [2]. Routing is the process of selecting a path through a network for the purpose of transmitting data from source to destination and it is a critical requirement for the proper functioning of multi-hop network systems. Recent years have seen a global upsurge in the use of mobile devices, which has also accentuated the critical requirement of having secure routing frameworks for MANETs in order to maintain the confidentiality and integrity of mobile devices [2].

Security in MANETs during routing has posed a great challenge to its effectiveness and utilization especially for security-sensitive applications. In securing an ad hoc network, consideration is given to the following network attributes: availability, authentication, integrity, confidentiality, and nonrepudiation. The various characteristics of ad hoc networks, such as, their open network design, the shared wireless medium they use, scarce resource constraints and the extremely dynamic network topology, make these networks vulnerable to different routing attacks like, modification attacks, fabrication attacks, spoofing attacks and rushing attacks. All these and more pose significant challenges to effective routing in ad hoc networks [3]. Although, research on secure routing in MANETs has attracted significant attention from researchers worldwide for more than a decade now, it has still remained an interesting research area [7-10]. Among the different secure routing mechanisms proposed, trust-based secure routing protocols for MANETs have gained great importance among researchers. In line with that, this paper proposes Grade Trust, a secure trust level routing protocol for MANETs. Grade Trust isolates excessive routing computations while minimizing communication overheads.

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. 4, Issue 10, October 2016

II. SECURE TRUST BASED ROUTING: BACKGROUND STUDY

The nature of MANETs brings a plethora of security challenges that need to be addressed. The vulnerability of communication channels and nodes and the high mobility of the changing topology make the security of MANETs difficult to deal with. The wireless broadcast of messages and the injection of false information in the network allow eavesdropping to happen thereby compromising the confidentiality and integrity of the whole network [4]. Different countermeasures, such as, cryptographic or trust-based approaches are proposed by the research fraternity to secure routing protocols in MANETs. While, cryptographic approaches are able to prevent tampering of routing information, they cannot secure the nodes participating in routing. On the other hand, trust-based mechanisms are able to not only secure the nodes but also the transmission of data. Traditional MANET routing protocols like AODV and FSR are susceptible to a number of security attacks, which include, black hole and grey hole attacks, flooding and Sybil attacks. AODV is a reactive routing protocol that floods the network during network discovery. Routes are thus determined only when needed. AODV relies on route flooding to discover its neighbors resulting in significant network overheads on the resource constrained nodes. Its performance is also poor in large networks [5]. FSR (Fisheye State Routing) is a proactive routing protocol based on the Link State routing algorithm with an improved route overhead in maintaining network topology information [6]. In FSR, nodes exchange link state data specifically with their neighbors to maintain the current topology information. These link state updates are further interchanged among nodes and thus each node has full view of the network map. FSR scales well in large networks as it condenses the regularity of update packets to other nodes while sending messages to nearby nodes.

In MANETs, trust-based routing mechanisms make the protocols more secure. Trust can be defined as the affiliation between two parties, where one party (trustor) is ready to count on the (expected) actions performed by the second party (trustee). In other words, the trustor is the evaluator while the trustee is been evaluated to determine its trust level [7]. Secure trust level routing entails the development of a routing protocol with security features enshrined into it to provide routing efficiency among nodes. It also ensures that malicious nodes do not have an impact on the normal operations of the network. A number of secure trust-based routing protocols have been developed for MANETs and are presented below.

Trust Based Routing for Misbehavior Detection in Ad Hoc Networks [14]. A Trust based routing protocol which computes route request based on node experience and knowledge recommendation from neighbors. Routing request carries trust information in it while ensuring the selection of the route with the highest trust to detect and isolate a black hole attack. Malicious attacks such as wormhole, byzantine attacks are still possible and fabricating trust recommendation nodes can conspire within the network.

SRT-Secure Routing using Trust Levels in MANETs [15]. This trust based routing model is founded on beacons transmitted/ received while trust routing is performed by selecting the best node in the same trust level. This way a black hole attack is identified and isolated. Nevertheless, the protocol is susceptible to sink hole, wormhole attacks as trust values can be compromised.

III. GRADETRUST: A SECURE ROUTING PROTOCOL

This paper proposes a secure routing protocol for MANETs called Grade Trust, which uses trust levels among nodes to isolate malicious nodes perpetrating black hole attacks. It offers secure routing of data traffic and improved packet delivery ratio in MANETs through the selection of non-malicious and secure nodes based on trust computation. In a network running GradeTrust protocol, the ratio of the effective packet interchange between neighbor nodes in the network (i.e., number of packets received and transmitted) is computed. Based on this ratio, all the nodes in the network operating under the GradeTrust protocol are classified into three sets in order of importance as per the trust levels of the nodes. The first set of nodes are classified as TrustedFriends (tf) which are the much secure nodes. The next set of nodes are classified as Friends (f) and are moderately secure. Lastly, the remaining nodes, which are not very secured, are classified as Possible Friends (pf). The nodes in the network are further sorted in declining order of their computed trust values and the top one third of the nodes (i.e., the Trusted Friends) are graded as 3, the Friends are graded as 2 and the remaining Possible Friends are graded as 1. During routing, a source node selects the next hop from its Trusted Friends (which is a set of the best neighbors with the same trust level of categories defined) and forwards the request ahead. This process continues until the packet reaches the destination. In comparison to AODV and FSR, Grade Trust ensures efficient route selection and packet delivery while mitigating the black hole attacks. Even in the absence of

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. 4, Issue 10, October 2016

such attacks Grade Trust does not impose any undue overhead on packet processing and transmission. This protocol ensures the establishment of secure and authenticated route for data transfer.

A.FUNCTIONING OF GRADETRUST PROTOCOL

The trust level of each node is based on the successful packet interchange between nodes. A satisfactory packet interchange ratio in Grade Trust reflects the level of satisfaction and trust among fellow nodes. This value, indicated by NS_{ij}, is used as a trust metric to compute and grade the trust levels of nodes. Depending on the trust level of nodes, those with high values (i.e., high level rating) are made available for secure routing while others with little or no trust value are avoided during secure routing. Network trust is, however, compromised if there are no neighbor nodes with a good trust value from the Trusted Friends category. In that case, Grade Trust computes a suitable alternative route by selecting a grade 2 node from the Friends category. In GradeTrust, every node that requests for packet transmission, checks the "grade" field in the neighbor's routing table to find out whether the destination node belongs to the same "grade". Provided it finds out the destination node, the sender transmits packets, else, it requests the next best neighbor of the node of same "grade". However, if no neighbor is found suitable, the trust is assumed to be compromised and hence, a neighbor located in the next lower level is chosen. If a destination is found in the next lower neighbor's table the search is terminated, else it is extended to its adjacent neighbors of the lower node chosen.

B.ROUTING USING GRADETRUST PROTOCOL

During route discovery involving the flooding of the network, the computation of trust rates is derived by:

$$NS_{ij} = \frac{S_{ij}}{C_{ij}} \quad \text{..... 1}$$

This also highlights effective packet interchange between neighbor nodes [15]. In equation 1, C_{ij} represents the number of requests sent to node j (N_j) from node i (N_i). S_{ij} represents the number of successful packet exchanges between N_i and N_j. N_i maintains a database of its neighbors and packets transmitted to them. For every request sent to N_j by N_i the C_{ij} is incremented by one. The effective packet exchange rate, NS_{ij}, between N_i and N_j is computed as given by (1).

C.COMPROMISE IN TRUST AMONG NODES

In GradeTrust, the trust metric, NS_{ij}, follows the below mentioned mechanism to enable the effective identification of malicious nodes. Trust compromise is computed based on the comparison of the total nodes in the lower levels with those at the source level. For a source node in the Trusted Friends (tf) list, if the node is considered malicious then its trust compromise is given by the total nodes in the Friends (f) list plus four times the number of nodes in the Possible Friends (pf) list. The idea here is to dissociate as quickly as possible a compromised node from other trusted nodes and thus pushing down the compromised node to the lower level (it becomes a likely untrusted node). This is represented as:

$$T_{comp} = (f + 4 * pf) \quad \text{..... 2}$$

Where:

f (Friends): Total nodes in the Friends list pf (Possible Friends): total nodes in the Possible Friends list.

IV. PERFORMANCE ANALYSIS

The GradeTrust protocol is simulated to validate and study its performance in comparison to two other well-known MANET routing protocols, namely, AODV and FSR. We detail below the simulation setup used to analyze Grade Trust's performance both in the presence and absence of black hole attacks. Three different performance metrics, namely, the packet-delivery ratio, the end-to-end delay and trust compromise among nodes, are considered for simulation. The obtained results are presented in the following sub-sections.

A.PERFOMANCE OF PROTOCOLS IN THE ABSENCE OF BLACKHOLE ATTACK

We measured the performance of all three protocols in the absence of black hole attacks. This is necessary in order to reveal whether our proposed solution has introduced some extra security processing overheads which may tend to deplete the resources of the nodes within the network.

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. 4, Issue 10, October 2016

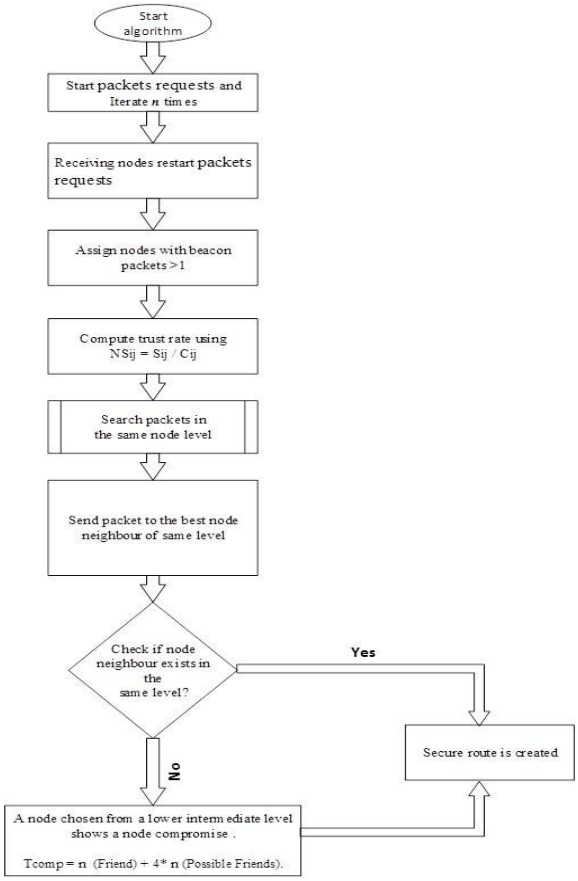

Fig. 1.Logical flow control for proposed GradeTrust protocol for black hole attack detection and isolation.

A. PACKET DELIVERY RATIO

This is defined as the amount of data packets generated by the constant bit rate (CBR) sources that are delivered to the destination. Packet delivery ratio (PDR) assesses the capability of the protocol to learn new routes. As per the results, the packet delivery ratio of GradeTrust protocol was 1.0% better than FSR and 1.4% better than AODV even when the node mobility was high. No malicious nodes are considered for this simulation. Referring to Section III, the nodes of GradeTrust system are placed at grade 3 in the network route resulting in an improved packet delivery ratio (PDR) in comparison to AODV and FSR.

B.END-TO-END DELAY

The performance results for end-to-end delay, which is the average delay encountered between the source and the destination node and is a result of delays occurring during route acquisition, buffering and processing at all adjoining nodes to the destination. It can be seen that at higher mobility levels GradeTrust, after 1,800 seconds of simulation run, had 14.6% reduced end to-end delay over FSR. This is because routing in GradeTrust is limited to nodes that fall within a specific trust grade.On the contrary, GradeTrust experienced a 37% higher end-to-end delay in comparison to AODV and this could be attributed to the extra security layer for secure network routing.

C. TRUST COMPROMISES AMONG NODES

Trust compromise reveals the vulnerability of the network to malicious attacks and is characterized by the number of lower grade nodes operating and maintaining secure routes. This is risky as most of these lower grade nodes have either been compromised or are highly vulnerable to malicious attacks. In GradeTrust, however, routes are selected by avoiding the paths where trust compromises are high. Thus, relatively secure routes are identified and used to create secure communication channel.

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. 4, Issue 10, October 2016

D. PERFOMANCE OF PROTOCOLS IN THE PRESENCE OF BLACKHOLE ATTACK

In this section, we present the simulation results of the performance of GradeTrust, FSR and AODV protocols in presence of black hole attack.

1)Packet Delivery Ratio (PDR)

It increase in speed of node mobility, overall there is a decrease in the packet delivery ratio. However, the PDR of GradeTrust is higher in comparison to FSR and AODV because GradeTrust is able to detect and isolate malicious nodes in the network. In GradeTrust, the packets are able to choose new routing paths via nodes with higher trust grades. Results show that the PDR of GradeTrust was 46% higher than AODV and 21.6% higher than FSR in the presence of black hole attack. This shows that AODV in the presence of black hole attack has the worst performance and unable to cope with black hole attack.

2)End-to-End Delay

It increase in end-to end delays for GradeTrust and FSR with the increase in node mobility. Similar to the results presented in Figure 4, end-to end delay for GradeTrust in this case as well is 46% higher than in AODV. This is due to the time consumed by GradeTrust in detecting and avoiding malicious nodes and establishing new secure routes using the trust grade within the network topology.

3)Trust Compromise

Comparison of the trust compromise levels for GradeTrust, FSR and AODV in the presence of black hole attacks is shown in Figure 8. According to the results, trust compromise in GradeTrust is lower than FSR and AODV protocols. This is primarily because memberships of most nodes in GradeTrust fall in grade 3 resulting in better efficiency in forwarding control packets in comparison to other lower grades.

V.CONCLUSION AND FUTURE WORK

This paper proposes, GradeTrust, a secure trust-based routing protocol that offers improved packet delivery ratios and enables secure routing of network traffic in MANETs. It isolates malicious nodes from the network using trust levels. Simulation studies, in the absence and presence of black hole attacks, have shown better performance results for GradeTrust in comparison to well-known traditional routing protocols like, AODV and FSR using different metrics including, packet delivery ratio, end-to-end delay and trust compromise. Future work on this research will further explore the potential of GradeTrust in detecting and isolating additional routing attacks

REFERENCES

[1]M. Ilyas, The handbook of ad hoc wireless networks. Boca Raton: CRC Press, 2003.
[2]D. Wang and P. Wang, "Understanding Security Failures of Two-Factor Authentication Schemes For Real-Time Applications In Hierarchical Wireless Sensor Networks," Ad Hoc Networks - Elsevier B.V.
[3]L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An Accurate and Precise Malicious Node Exclusion Mechanism For Ad Hoc Networks," Ad Hoc Networks
[4]S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications, Second Edition ed. Boca Raton
[5]C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing,"
[6]C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in INFOCOM, 2010
[7]S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security Vol. 5, 2007.
[8]L. Xiaoqi, M. R. Lyu, and L. Jiangchuan, "A trust model based routing protocol for secure ad hoc networks," in Aerospace Conference, 2004. Proceedings. 2004 IEEE, 2004.
[9]M. Al-Shurman and S.-M. Yoo, " Black Hole Attack in Mobile Ad Hoc Networks," in Annual Southeast Regional Conference 2004.