International Journal of Computer Applications Technology and Research
Volume 3– Issue 9, 536 - 540, 2014, ISSN: 2319–8656

Security improvements Zone Routing Protocol in Mobile Ad Hoc Network

Mahsa Seyyedtaj
Department of computer, Shabestar branch,
Islamic Azad University, Shabestar,
Iran

Mohammad Ali Jabraeil Jamali
Department of computer, Shabestar branch,
Islamic Azad University, Shabestar,
Iran

Abstract: The attractive features of ad-hoc networks such as dynamic topology, absence of central authorities and distributed cooperation hold the promise of revolutionizing the ad-hoc networks across a range of civil, scientific, military and industrial applications. However, these characteristics make ad-hoc networks vulnerable to different types of attacks and make implementing security in ad-hoc network a challenging task. Many secure routing protocols proposed for secure routing either active or reactive, however, both of these protocols have some limitations. Zone Routing Protocol (ZRP) combines the advantages of both proactive and reactive routing protocols. In this paper we analyze the ZRP security improvements. Considering the delivery rate of packets, routing overhead, network delay, Simulation results show that Protocols operate under different constraints and none of the protocols are not able to provide security for all purposes.

Keywords: ad-hoc networks; secure routing; secure neighbor discovery; digital signature; zone routing protocol; secure zone routing protocol

1. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among them-selves without the reliance on a fixed base station or a wired back-bone network. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. MANET is very useful to apply in different applications such as battlefield communication, emergency relief scenario etc. In MANET nodes are mobile in nature, due to the mobility, topology changes dynamically. Due to its basic Ad-Hoc nature, MANET is venerable to various kinds of security attacks [1].

Researchers have proposed a large range of routing protocols for ad hoc networks. The basic goals of these protocols are the same: maximize throughput while minimizing packet loss, control overhead and energy usage. However, the relative priorities of these criteria differ among application areas. In addition, in some applications, ad hoc networking is really the only feasible solution, while in other applications, ad hoc networking competes with other technologies. Thus, the performance expectations of the ad hoc networks differ from application to application and the architecture of the ad hoc network, thus each application area and ad hoc network type must be evaluated against a different set of metrics. The routing protocols have organized into nine categories based on their underlying architectural framework as follows [2].

- Source-initiated (Reactive or on-demand)
- Table-driven (Pro-active)
- Hybrid
- Location-aware (Geographical)
- Multipath
- Hierarchical
- Multicast
- Geographical Multicast
- Power-aware

Among these protocols, refer to the first three:

Reactive Routing protocols: Whenever there is a need of a path from any source to destination then a type of query reply dialog does the work.Therefore, the latency is high; however, no unnecessary control messages are required.

Proactive routing protocols: In it, all the nodes continuously search for routing information with in a network, so that when a route is needed, the route is already known. If any node wants to send any information to another node, path is known, therefore, latency is low. However, when there is a lot of node movement then the cost of maintaining all topology information is very high.

Hybrid routing protocols: These protocols incorporates the merits of proactive as well as reactive routing protocols. A hybrid routing protocol should use a mixture of both proactive and reactive e approaches. Hence, in the recent years, several hybrid routing protocols are proposed like ZRP [5].

1.1 ZRP

Zone routing protocol is a hybrid protocol. It combines the advantages of both proactive and reactive routing protocols. A routing zone is defined for every node. Each node specifies a zone radius in terms of hops. Zones can be overlapped and size of a zone affects the network performance. The large routing zones are appropriate in situations where route demand is high and /or the network consists of many slowly moving nodes. On the other hand, the smaller routing zones are preferred where demand for routes is less and /or the network consists of a small number of nodes that move fast relative to one another. Proactive routing protocol works with in the zone whereas; reactive routing protocol works between the zones. ZRP consists of three components:

1) the proactive Intra zone routing protocol (IARP)

2) the reactive Inter zone routing protocol (IERP)

3) Bordercast resolution protocol (BRP).

Each component works independently of the other and they may use different technologies in order to maximize efficiency in their particular area. The main role of IARP is to ensure that every node with in the zone has a consistent updated routing table that has the information of route to all the destination nodes with in the network. The work of IERP gets started when destination is not available with in the zone. It relies on bordercast resolution protocol in the sense that border nodes will perform on-demand routing to search for routing information to nodes residing outside the source node zone [6]. The architectural of ZRP is shown in Figure 1.

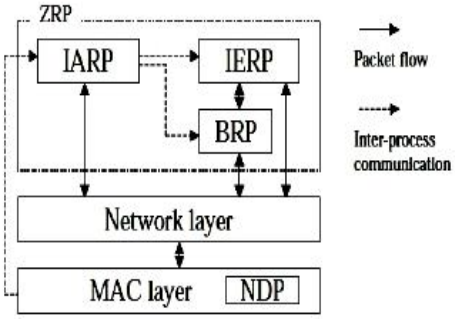

Figure 1. Architecture of ZRP [6].

2. PREVIOUS WORKS

In this section security improvements ZRP have examined.

2.1 SZRP1

The architectural design of SZRP1 is shown in Figure 2. The proposed architecture is a modification of ZRP [4]. It is designed to support both secure routing (intrazone and interzone) and effective key management. There are dedicated and independent components in SZRP1 to carry out these tasks. The functionality of each component and their interrelationship is explained below.

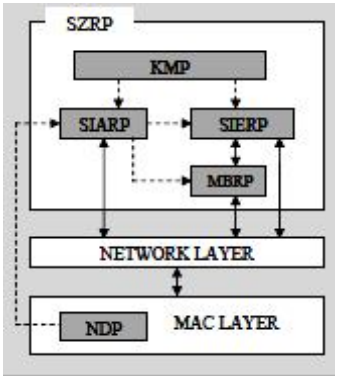

Figure 2. Architecture of SZRP1[4].

The key management protocol (KMP) is responsible for public key certification process. It fetches the public keys for each CN by certifying them with the nearest CA. The secure intrazone routing protocol (SIARP) and secure interzone routing protocol (SIERP) uses these keys to perform secure intrazone and interzone routing respectively.

SIARP is a limited depth proactive link-state routing protocol with inbuilt security features. It periodically computes the route to all intrazone nodes (nodes that are within the routing zone of a node) and maintains this information in a data structure called SIARP routing table. This process is called proactive route computation. The route information to all intrazone nodes collected in proactive route computation phase is used by SIARP to perform secure intrazone routing.

SIERP is a family of reactive routing protocols with added security features like ARAN. It offers on demand secure route discovery and route maintenance services based on local connectivity information monitored by SIARP.

In order to detect the neighbor nodes and possible link failures, SZRP relies on the neighborhood discovery protocol (NDP) similar to that of ZRP. NDP does this by periodically transmitting a HELLO beckon (a small packet) to the neighbors at each node and updating the neighbor table on receiving similar HELLO beckons from the neighbors. NDP gives the information about the neighbors to SIARP and also notifies SIARP when the neighbor table updates. We have assumed that NDP is implemented as a MAC layer protocol. A number of security mechanisms suggested in for MAC layer can be employed to secure NDP.

To minimize the delay during interzone route discovery, SIERP uses bordercasting technique similar to ZRP, which is implemented here by the modified border resolution protocol (MBRP). MBRP is a modification of the bordercast technique adopted in ZRP. It not only forwards SIERP's secure route discovery packets to the peripheral nodes of the bordercasting node but also sets up a reverse path back to the neighbour by recording its IP address. MBRP uses the routing table of SIARP to guide these route queries. Since, all security measures are taken by SIERP during interzone routing; no additional security mechanism is adopted by MBRP during bordercasting.

2.1.1 Simulation Environment

The simulation of Secure Zone Routing Protocol (SZRP) was conducted in NS-allinone-2.1b6a, on an Intel Pentium IV processor (2.4 GHz) and 512 MB of RAM running Ubuntu 7.2.

2.1.2 Performance Metrics

four performance metrics evaluated to compare the proposed protocol with ZRP under a trusted environment where all the nodes in the network are assumed to be benign. They are discussed below:

Average packet delivery fraction: This is the fraction of the data packets generated by the CBR sources that are delivered to the destination. This metric is important as it evaluates the ability of the protocol to discover routes.

Average routing load in bytes: This is the ratio of overhead control bytes to delivered data bytes. Secure Zone Routing Protocol (SZRP) has larger control overhead due to the certificate and signature embedded in the packets. For the calculation of this metric, the transmission at each hop along the route was counted as one transmission.

Average routing load in terms of packets: This metric is similar to the above, but here the ratio of control packet overhead to data packet overhead is calculated.

Average route acquisition latency: This is the average delay between the sending of a secure route discovery packet by a source for discovering a route to a destination and the receipt of the first corresponding route reply. This includes all the delays caused during the route discovery and route reply phases for signature verification and their replacement, in addition to the normal processing of the packets. If a route request timed out and needed to be retransmitted, the sending time of the first transmission was used for calculating the latency.

2.1.3 Simulation Environment

To evaluate proposed SZRP in a non-adversarial environment, the Network Simulator 2 (NS-2) have used. NS-2 is a discrete event simulator written in C++ and OTcl. At the link layer, the simulator implements the complete IEEE 802.11 standard Medium Access Control (MAC) protocol.

2.1.4 Simulation Results

In this section, The obtained results analyzed for each of the performance metric discussed. The resulting data were plotted using Gnuplot. Each data point in the resulting graphs is an average of 5 simulation runs with identical configuration but different randomly generated mobility patterns.

2.1.4.1 Average Packet Delivery Fraction

obtained results for average packet delivery fraction for both the 10 and 20 node networks. The packet delivery fraction obtained using SZRP is above 96% in all scenarios and almost identical to that obtained using ZRP. This suggests that SZRP is highly effective in discovering and maintaining routes for delivery of data packets, even with relatively high node mobility.

2.1.4.2 Average Routing Load in Bytes

The routing load measurements for both the protocols in terms of number of control bytes per data bytes delivered. The byte routing load of Secure Zone Routing Protocol (SZRP) is higher compared to that of ZRP. For example, it is nearly 40% for 20 nodes moving at 5 m/s, as compared to 22% for ZRP with identical topology and mobility pattern. With further increase in node mobility to 10 m/s, it increases to 75%, compared 45% for ZRP. This overhead is due to the certificate and signature embedded in the packets. The RSA digital signature is of 16 bytes and the certificate is 512 bytes long. Though these extra bytes are pure overhead they are necessary for security provisioning. Additionally, since ZRP has the advantage of smaller sized packets, the packet size of SZRP is not that much larger compared to other secure routing protocols even after inserting the security data.

2.1.4.3 Average Routing Load in Terms of Packets

While the number of control bytes transmitted by SZRP is larger than that of ZRP, the number of control packets transmitted by the two protocols is roughly equivalent. Figure 5.5 shows the average number of control packet transmitted per delivered data packet. Except for the scenario of 20 nodes moving at 1 m/s, where they exhibit some difference, the packet routing load for both the protocols are nearly the same for other scenarios. This is due to the fact that SZRP did not employ any extra control packets compared to ZRP for secure routing, except for the case of intrazone routing, which requires two additional control packets SKREQ and SKREP. However, with high node mobility, for example, when the nodes move with the speed of 5 m/s or 10 m/s, the number of times interzone routing carried out was significantly higher than intrazone routing. In this respect, the two protocols demonstrate nearly the same amount of packet overhead.

2.1.4.4 Average Route Acquisition Latency

The average route acquisition latency for Secure Zone Routing Protocol (SZRP) is approximately 1.7 times as that of ZRP. For example, for 10 nodes moving at 5 m/s, it is 60ms as compared to 100ms for ZRP, while for 20 nodes moving at 10 m/s, it is nearly 135ms as compared to 75ms as in the case of ZRP. While processing SZRP routing control packets, each node has to verify the digital signature of the previous node, and then replace this with its own digital signature, in addition to the normal processing of the packet as done by ZRP. This signature generation and verification causes additional delays at each hop, and so the route acquisition latency increases [4].

2.2 SZRP2

The architectural design of SZRP2 is shown in Figure 3 that modified it by using four stages. First, an efficient key management mechanism used that is considered as a prerequisite for any security mechanism. Then, a secure neighbor detection scheme provided that relies on neighbor discovery, time and location based protocols. Securing routing packets is considered as the third stage which depends on verifying the authenticity of the sender and the integrity of the packets received. Finally, detection of malicious nodes mechanism is used to identify misbehaving nodes and isolate them using blacklist. Once these goals are achieved, providing confidentiality of transferred data becomes an easy task which can be implemented using any cryptography system [3].

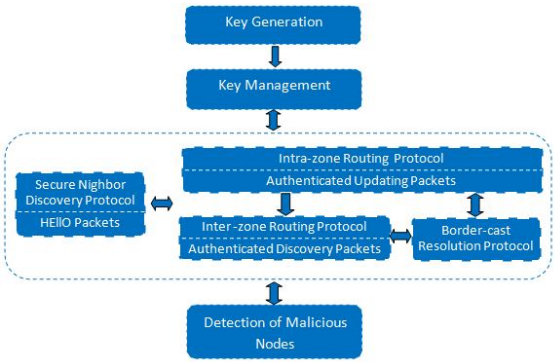

Figure 3. Architecture of SZRP2[3].

2.2.1 Performance Metrics

proposed protocol evaluated by comparing it with the current version of ZRP. Both protocols are run on identical movements and communication scenarios; the primary metrics used for evaluating the performance of SZRP are packet delivery ratio, routing overhead in bytes, routing overhead in packets, and end-to-end latency. These metrics are obtained from enhancing the trace files.

Packet delivery ratio: This is the fraction of the data packets generated by the CBR sources to those delivered to the destination. This evaluates the ability of the protocol to discover routes.

Routing overhead (bytes): This is the ratio of overhead bytes to the delivered data bytes. The transmission at each hop along the route is counted as one transmission in the calculation of this metric. The routing overhead of a simulation run is calculated as the number of routing bytes generated by the routing agent of all the nodes in the simulation run. This metric has a high value in secure protocols due to the hash value or signature stored in the packet.

Routing overhead (packets): This is the ratio of control packet overhead to data packet overhead over all hops. It differs from the routing overhead in bytes since in MANETs if the messages are too large, they will be split into several packets. This metric is always high even in unsecure routing protocols due to control packets used to discover or maintain routes such as IARP and IERP packets.

Average End-to-End latency: This is the average delay between the sending of data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes [3].

2.2.2 Simulation Results

proposed SZRP simulated over four scenarios to evaluate it through different movement patterns, network size, transmission rate, and radius of the zone.

2.2.2.1 Performance against Different Mobility Networks

In this scenario, The SZRP and ZRP compared over different values of the pause time. The pause time was changed from 100 s to 500 s to simulate high and low mobility networks. Concerning the packet delivery ratio as a function of pause time, the result shows that the packet delivery ratio obtained using SZRP is above 90% in all scenarios and almost similar to the performance of ZRP. This indicates that the SZRP is highly effective in discovering and maintaining routes for the delivery of data packets, even with relatively high mobility network (low pause time). A network with high mobility nodes has a lower packet delivery ratio because nodes change their location through transmitting data packets that have the predetermined path. For this reason, a high mobility network has a high number of dropped packets due to TTL expiration or link break. For the extra routing overhead introduced by both SZRP and ZRP, where the routing overhead is measured in bytes for both protocols, the results show that the routing overhead of SZRP is significantly higher and increased to nearly 42% for a high mobility network and 27% for a low mobility network. This is due to the increase in size of each packet from the addition of the digest and the signature stored in the packets to verify the integrity and authentication. This routing overhead decreases as the mobility decreases due to increase of the number of updating packets required to keep track of the changes in the topology in order to maintain routing table up-to-date. These packets include both IARP and IERP packets as well as the error messages.

2.2.2.2 Performance against Different Data Rates and Mobility Patterns

In this scenario, The SZRP and ZRP compared over different values of data rate. These values considered since high data rate is always an imperative need in any network although it has an extreme effect in increasing the congestion in MANETs. The data rate was changed from one to nine packets per second. These scenarios are performed under high and low mobility networks, 100 s and 500 s, respectively. Fig. 4 shows the packet delivery ratio of SZRP and ZRP for both low and high mobility networks. We note that the packet delivery ratio exceeds 89% in all cases which can be considered as a good indicator that SZRP goes in the same manner as the conventional ZRP. The delivery packet ratio of low mobility networks increases as the data rate increases as expected since the discovered route to the destination will not change during transmitting the packets, and thus the success of delivering the packet to the same destination will increase. On the other hand, the packet delivery ratio decreases in high mobility networks as the data rate increases because of the high probability of congestion by both the increased data packets and the increased control messages needed to maintain the network nodes up-to-date with the changeable topology.

2.2.2.3 Performance against Different Network Sizes and Mobility Patterns

The third scenario studies the performance of SZRP and ZRP over different network sizes. The number of nodes changes from ten to forty in order to validate our secure routing protocol in different networks. The experiments are performed under high and low mobility rates with data rate of five packets per second. To be consistent, the dimension of the topology used is changed with the same ratio as the number of mobile nodes. The SZRP still performs well in low mobility network where it exceeds 99%. However, its performance degrades in a high mobility network. In both cases, the result obtained is accepted because it degrades in the same manner as the conventional ZRP. A final point observed from this figure is that the packet delivery ratio decreases in a large network which is an expected result due to the increase of the traveling time that may lead to TTL expiration.

2.2.2.4 Performance against Different Routing Zones and Mobility Patterns

The last scenario studies the performance of both protocols under different routing zones. The number of routing zone nodes can be regulated through adjustments in each node's transmitter power. To provide adequate network reachability, it is important that a node is connected to a sufficient number of neighbors. However, more is not necessarily better. As the transmitters' coverage areas grow larger, so do the embership of the routing zones, an excessive amount of update traffic

may result [3].

3. CONCLUSION

The paper conducted a survey on the two various security improvements suggested for ZRP. An analysis is conducted on each improvement and the applications which best suits each enhancement is suggested. All protocols in standard mode, In terms of the network performance are acceptable. But there are some security problems. To solve these security problems for each of these algorithms, an extension is proposed. The extensions of the protocol's security problems have been resolved, But in terms of network performance problems have developed. Thus presentation an algorithm for ad hoc networks, both in terms of security and in terms of network performance is acceptable, it seems necessary. In evaluating the performance of both secure protocols, The results show that by increasing the routing overhead and average delay, packet delivery rate than the standard protocol is better. Both secure protocols to thwart further attacks at the network layer are suitable. The disadvantages of these two protocols failure to detect some attacks, such as jamming attack at the physical layer and the computational overhead is high.

According to Previous studies have reached conclude That all security protocols operate under different constraints and none of the protocols are not able to provide security for all purposes. Thus the design of new secure routing protocols against multiple attacks and to reduce the processing time in the process of identifying the problem still remains challenging.

4. REFERENCES

[1] Boora, S. et. al (2011). A Survey on Security Issues in Mobile Ad-Hoc Networks, International Journal of Computer Science & Management Studies, Vol. 11, Issue 02.

[2] Boukerche, A. et. al (2011). Routing protocols in ad hoc networks: A survey, Elsevier Computer Networks Journal, Vol. 55, Issue 13.

[3] Ibrahim, S. I. et. al (2012). Securing Zone Routing Protocol in Ad-Hoc Networks. I. J. Computer Network and Information Security, 10, 24-36.

[4] Kumar Pani, N. (2009) .A Secure Zone-Based Routing Protocol For Mobile Adhoc Network, thesis.

[5] Parvathavarthini, A. et. al (2013). An Overview of Routing Protocols in Mobile Ad-Hoc Network, International Journal of Advanced Research in Computer Science and Software Engg 3(2), February - 2013, pp. 251-259.

[6] Sudarsan, D. et. al (2012). A survey on various improvements of hybrid zone routing protocol in MANET, International Conference on Advances in Computing, Communications and Informatics Pages 1261-1265.