Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Fast and Secure Routing Protocol in Manet

By Vivek Anand Singh & Vineet Yadav
Shri Ramswaroop Memorial College, India

Abstract - This paper proposes an enhanced mobile ad-hoc routing protocol FSR (Fast and Secure Routing), which is enhanced version of best features of ZBR (Zone Based routing Protocol). FSR deals with speed and security both at the same time. The ZBR enhances the speed of the network whether TCP has provided the primary means to transfer data reliably across the Internet. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Early detection protocols have tried to address this problem with a user-defined threshold, the finding of detecting and removing compromised routers can be thought of as an instance of anomalous behaviour based intrusion detection. That can be the compromised router can that identified by correct routers when it deviates from exhibiting expected behaviour. This protocol can be evaluated in a small experimental network.

Keywords : *MANET, BGP (broader gateway protocol), ZBR (zone based routing), TCP, protocol X, TV (traffic validation).*

GJCST-E Classification : *C.2.5*

Strictly as per the compliance and regulations of:

Fast and Secure Routing Protocol in Manet

Vivek Anand Singh [α] & Vineet Yadav [σ]

Abstract - This paper proposes an enhanced mobile ad-hoc routing protocol FSR (Fast and Secure Routing), which is enhanced version of best features of ZBR (Zone Based routing Protocol). FSR deals with speed and security both at the same time. The ZBR enhances the speed of the network whether TCP has provided the primary means to transfer data reliably across the Internet. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Early detection protocols have tried to address this problem with a user-defined threshold, the finding of detecting and removing compromised routers can be thought of as an instance of anomalous behaviour based intrusion detection. That can be the compromised router can that identified by correct routers when it deviates from exhibiting expected behaviour. This protocol can be evaluated in a small experimental network.

Keywords : MANET, BGP (broader gateway protocol), ZBR (zone based routing), TCP, protocol X, TV (traffic validation).

I. Introduction

Active research work for MANETs is carrying on mainly in the fields of Medium Access Control (MAC), routing, resource management, power control, and security. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of MANET routing protocols have been proposed in the last few years. Considering the special properties of MANET, when thinking about any routing protocol, generally the following properties are expected, though all of these might not be possible to incorporate in a single solution.

- A routing protocol for MANET should be distributed in manner in order to increase its reliability.
- The routing protocol should consider its security.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A routing protocol must be designed considering unidirectional links because wireless medium may cause a wireless link to be opened in one direction only due to physical factors.
- A routing protocol should be aware of Quality of Service.
- The routing protocol should be power-efficient.

Author α σ : Shri Ramswaroop Memorial College of Engineering and Management, Uttar Pradesh, India. E-mails : vcyrus90@gmail.com, vineetabhiraaj@gmail.com

II. Previous and Related Work

Previous work on TCP and ZBR is as follows-

ZBR -ZBR combines the proactive and reactive routing approaches. It divides the network into routing zones. The routing zone of a node X includes all nodes within hop distance at most d from node X. All nodes at hop distance exactly d are said to be the peripheral nodes of node X's routing zone. The parameter d is the zone radius. ZBR proactively maintains the routes within the routing zones and reactively searches for routes to destinations beyond a node's routing zone. Route discovery is similar to that in DSR with the difference that route requests are propagated only via peripheral nodes. ZBR can be dynamically configured to a particular network through adjustment of the parameter d. ZBR will be a purely reactive routing protocol when d = 0 and a purely proactive routing protocol when d is set to the diameter of the network. ZBR discovers routes as follows. When a source node wants to send data to a destination, it first checks whether or not the destination is within its routing zone. If it is, then a route can be obtained directly. Otherwise, it floods a route request to its peripheral nodes. The peripheral nodes in turn execute the same algorithm to check whether the destination is within their routing zone. If it is, a route reply message is sent back to the source. Otherwise, the peripheral node floods the route request to its peripheral nodes again. This procedure is repeated until a route is found.

TCP-TCP is used for transmission services in ZBR which has provided the primary means to transfer data reliably across the Internet; however TCP has imposed limitation on several applications. Measurement and estimation of packet loss characteristics are challenging due to the relatively rare occurrence and typically short duration of packet loss episodes. While active probe tools are commonly used to measure packet loss on end-to end paths, there has been little analysis of the accuracy of these tools or their impact on the network. The main objective is to understand the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular to this concern a simple yet effective attack in which a router selectively drops packets destined for some Victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect .Such attacks are not mere theoretical curiosities, but they are actively employed in

practice. Attackers have repeatedly demonstrated their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords and latent software vulnerabilities. One network operator recently documented Over 5,000 compromised routers as well as an underground market for trading Access to them several researchers has developed.

III. Proposed Protocol Technique

Our project`s main objective is to remove the vulnerability in the ad-hoc network due to compromised routers and reducing delay generated due to route discovery. The FSR (Fast and Secure Routing) protocol is Combination of best features of TCP and ZBR which results in very efficient and secure network configuration. Since there is no central node in ad-hoc network in other words all nodes are mobile. Routing zone is determined by setting a zone radius (represented by parameter d) from a certain node. Peripheral nodes from that node form a routing zone.

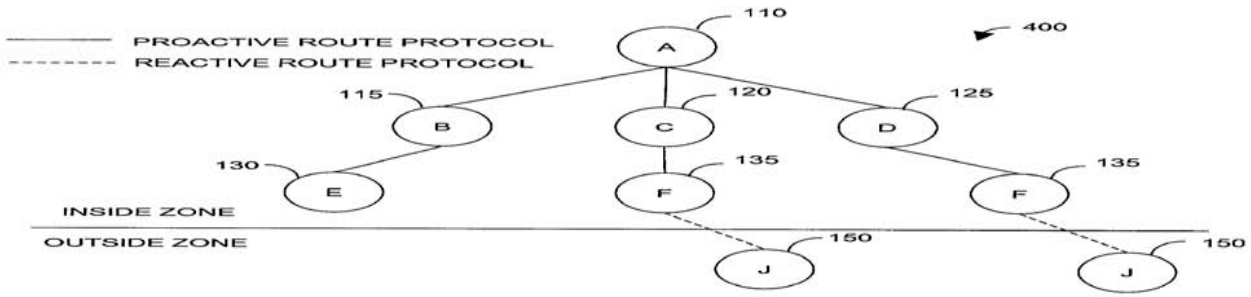

Figure 1 : Working of proactive and reactive routing protocol

The FSR works on algorithm which comprises of three modes and switches between first mode and second mode according to network demand which is implementation of ZBR. Third mode is always applicable. Functions of these three modes are as follows:

- In first mode, the FSR proactively maintains the route within the routing zone.
- In Second mode, FSR reactively searches for routes to destinations beyond a node's routing zone. Dynamic configuration of FSR is possible as it inherits ZBR features.
- In the Third mode, we set a deterministic behaviour for all routers in all routing zones by using TCP security policies and if any router deviates from this behaviour that is considered to be malicious. All packets incoming from malicious router will be dropped and another interface from that zone will be selected for communication. This action will prevent any loss of packets in network.

The concept discussed above can be implemented using "protocol X" and ZBR. Considering this scenario if any router will be compromised by the attacker that will be automatically identified and blocked in the network. In other scenario if there will be any increase in network traffic that will be managed by ZBR configuration and hence result in great reduction in network overhead and delay of packets. So, this is how we can implement a fast and secure routing.

a) MODE 1- Maintaining routes proactively

In order to maintain correct route information proactively, a node must periodically send control messages. Therefore, proactive routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no data traffic. The main advantage of this category of protocols is that hosts can quickly obtain route information and quickly establish a session.

For Example: GSR introduced below is a proactive routing protocol.

Global State Routing (GSR) is based on the Link State (LS) routing method. In the LS routing method, each node floods the link state information into the whole network (global flooding) once it realises that links change between itself and its neighbours. The link state information includes the delay to each of its neighbours. A node will know the whole topology when it obtains all link information. LS routing works well in networks with static topologies. When links change quickly, however, frequent global flooding will inevitably lead to huge control overhead. Unlike the traditional LS method, GSR does not flood the link state packets. Instead, every node maintains the link state table based on up-to-date LS information received from neighbouring nodes, and periodically exchanges its LS information with its neighbours only (no global flooding). Before sending an LS packet, a node assigns the LS packet a unique sequence number to identify the newest LS information. LS information is disseminated as the LS packets with larger sequence numbers replace the ones with smaller sequence numbers.

The convergence time required to detect a link change in GSR is shorter than in the Distributed Bellman-Ford (DBF) protocol. The convergence time in GSR is O(D*I) where D is the diameter of the network and I is the link state update interval. The convergence time is normally smaller than O(N*I) in DBF, where N is

the number of nodes in the networks and I is the update interval. Since the global topology is maintained in every node, preventing routing loops is simple and easy.

The drawbacks of GSR are the large size of the update messages, which consume a considerable amount of bandwidth, and the latency of the LS information propagation, which depends on the LS information update interval time. ``Fisheye'' technology can be used to reduce the size of update messages. In this case, every node maintains highly accurate network information about the immediate neighbouring nodes, with progressively fewer details about farther nodes.

b) MODE 2- Searching routes to destination reactively

Reactive routing protocols can dramatically reduce routing overhead because they do not need to search for and maintain the routes on which there is no data traffic. This property is very appealing in the resource-limited environment.

i. *Ad hoc On-Demand Distance Vector (AODV) Routing*

Since DSR includes the entire route information in the data packet header, it may waste bandwidth and degrade performance, especially when the data contents in a packet are small. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve performance by keeping the routing information in each node. The main difference between AODV and DSR is that DSR uses source routing while AODV uses forwarding tables at each node. In AODV, the route is calculated hop by hop. Therefore, the data packet need not include the total path.

The route discovery mechanism in AODV is very similar to that in DSR. In AODV, any node will establish a reverse path pointing toward the source when it receives an RREQ packet. When the desired destination or an intermediate node has a fresh route (based on the destination sequence number) to the destination, the destination/intermediate node responds by sending a route reply (RREP) packet back to the source node using the reverse path established when the RREQ was forwarded. When a node receives the RREP, it establishes a forward path pointing to the destination. The path from the source to the destination is established when the source receives the RREP.

For example: Dealing with path failures in AODV is more complicated than in DSR. When a node detects the link failure to its next hop, it propagates a link failure notification message (an RREP with a very large hop count value to the destination) to each of its active upstream neighbours to inform them to erase that part of the route. These nodes in turn propagate the link failure notification message to their upstream neighbours, and so on, until the source node is reached. A neighbour is considered active for a route entry if the neighbour sends a packet, which was forwarded using that entry, within the active-route-timeout interval. Note that the link failure notification message will also update the destination sequence number. When the source node receives the link failure notification message, it will re-initiate a route discovery for the destination if a route is still needed. A new destination sequence number is used to prevent routing loops formed by the entangling of stale and newly established paths.

AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information. As in DSR, the response time may be large if the source node's routing table has no entry to the destination and thus must discover a path before message transmission. Furthermore, the same problems exist as in DSR when network partitions occur.

c) MODE 3- Securing network

i. *Protocol X*

The Protocol x detects traffic faulty routers by validating the queue of each output interface for each router. Given the buffer size and the rate at which traffic enters and exits a queue, the behaviour of the queue is deterministic. If the actual behaviour deviates from the predicted behaviour, then a failure has occurred. We present the failure detection protocol in terms of the solutions of the distinct sub-problems: traffic validation, distributed detection, response, and the correctness of the protocol.

ii. *Traffic Validation Correctness*

The Traffic validation of the failure of detecting malicious attack by TV results in a false negative, and any misdetection of legitimate behaviour by TV results in a false positive. Within the given system model of Section the example TV predicate is correct. However, the system model is still simplistic. In a real router, packets may be legitimately dropped due to reasons other than congestion errors in hardware, software or memory, and transient link errors. Classifying these as arising from a router being compromised might be a problem, especially if they are infrequent enough that they would be best ignored rather than warranting repairs the router or link. A larger concern is the simple way that a router is modelled in how it internally multiplexes packets. This model is used to compute time stamps. If the time stamps are incorrect, then TV could decide incorrectly. We hypothesize that a sufficiently accurate timing model of a router is attainable but have yet to show this to be the case. A third concern is with clock synchronization. This version of TV requires that all the routers feeding a queue have synchronized clocks. This requirement is needed in order to ensure that the packets are interleaved correctly by the model of the router. The synchronization requirement is not necessarily daunting; the tight synchronization is only required by routers adjacent to the same router. With low-level time stamping of packets and repeated exchanges of time it should be straightforward to synchronize the clocks sufficiently

tightly. Other representations of collected traffic information and TV that we have considered has their own problems with false positives and false negatives. It is an open question as to the best way to represent TV. We suspect any representation will admit some false positives or false negatives.

IV. Conclusion

In this paper, we propose an adaptive algorithm which adapts itself according to network demand by maintaining balance between zones based routing (ZBR) and transmission control protocol (TCP). Routes are maintained proactively in routing zone and Route discovery is done using reactive protocol. While faulty routers are detected by using protocol x by setting a constant buffer size and deterministic behaviour of queue at which traffic enters and exits. Proactive routing is done using global state routing (GSR) which is based on the Link State (LS) routing method. The link state information includes the delay to each of its neighbours. A node will know the whole topology when it obtains all link information. While reactive routing is done using Ad-hoc on demand Vector (AODV) routing. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve performance by keeping the routing information in each node. AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information. Thus the overall algorithm brings efficiency and reliability in MANET.

References Références Referencias

1. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994: 234–244.
2. Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989). A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4: 224–236.
3. Murthy S, Garcia-Luna-Aceves JJ (1996). An Efficient Routing Protocol for Wireless Networks. Mobile Networks and Applications, Volume 1, Issue 2:183–197 ISSN: 0975-3397 711 G. Vijaya Kumar et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713.
4. Humblet PA (1991) another Adaptive Distributed Shortest-Path Algorithm. IEEE Transactions on Communications, Volume 39, Issue 6: 995–1003.
5. Rajagopalan B, Faiman M (1991). A Responsive Distributed Shortest-Path Routing Algorithm With in Autonomous Systems. Journal of Internetworking Research and Experiment, Volume 2, Issu.
6. R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog org/mtg-0306/pdf/thomas.pdf, June 2003.
7. K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Ols- son, "Detecting Disruptive Routers: A Distributed Network Monitoring Approach," Proc. IEEE Symp. Security and Privacy (S&P '98), pp. 115-124, May 1998.
8. A.T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, "Detecting and Isolating Malicious Routers," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 3, pp. 230-244, July-Sept. 2006.
9. L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, "Listen and Whisper: Security Mechanisms for BGP," Proc. First Symp. Networked Systems Design and Implementation (NSDI '04), Mar. 2004.
10. S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gate- way Protocol (Secure-BGP)," IEEE J. Selected Areas in Comm., vol. 18, no. 4, pp. 582-592, Apr. 2000.
11. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. ACM MobiCom' 02, Sept. 2002.
12. B.R. Smith and J. Garcia-Luna-Aceves, "Securing the Border Gate- way Routing Protocol," Proc. IEEE Global Internet, Nov. 1996.
13. S. Cheung, "An Efficient Message Authentication Scheme for Link State Routing," Proc. 13th Ann. Computer Security Applications Conf. (ACSAC '97), pp. 90-98, 1997.
14. M.T. Goodrich, Efficient and Secure Network Routing Algorithms, provisional patent filing, Jan. 2001.
15. R. Perlman, "Network Layer Protocols with Byzantine Robust-ness," PhD dissertation, MIT LCS TR-429, Oct. 1988.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org