www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10529-10532

On Demand Load Balance Secure Routing Scheme For Mobile ADHOC Network

Shishir Patra[1] Jajati Mallick[2]
Department of Computer Science and Engineering
Purushottam Institute of Engineering and Technology
Rourkela, Mandiakudar, Odisha, India
shishirpatra9@gmail.com[1]
mallick.jajati@gmail.com[2]

Abstract: ***Mobile Adhoc Network (MANET) is a special type of wireless network. It is characterized by dynamic topology (infrastructure less), multi-hop communication, limited resources (bandwidth, CPU, battery, etc.) and limited security. In this paper, we focus on the situation that occurs when specialized, sensitive data are sent to the Internet from MANET nodes. These special data types are especially susceptible to security risks such as information leak and data falsification. Therefore, it is necessary for such special data to be forwarded by a secure/trusted gateway which is under control of a trusted network administrator. However, there can be multiple gateways deployed in a MANET, where the cost ineffectiveness makes it difficult for a network administrator to simultaneously manage every gateway. An optimum mechanism is used to select an appropriate gateway out of the multiple gateways based on multiple node metrics: remaining energy and gateway load for interconnected Mobile Ad hoc Network (MANET) with infrastructure network. To choose an optimum gateway node, we use the Multiple Criteria Decision Making (MCDM) method called Simple Additive Weighting (SAW) for the optimum gateway node. SAW method calculates the weights of gateway node by considering these two metrics. Node with the highest weight will be selected as a gateway. Because of the risk of forwarding special data through an unmaintained gateway, we propose a routing protocol, which allows a source node to have all data forwarded to the Internet through a trusted gateway. To achieve the desirable performance, we have implemented routing protocol called Dynamic MANET On demand (DYMO), which works in consideration of application data. Through simulations, we evaluate our protocol in comparison with the conventional DYMO protocol. We conclude through the simulation results that our protocol get better performance in terms of packet delivery ratio and transmission delay.***

Keywords: Gateway; Integration; MANET; Routing Protocol; Selection; Security

1. INTRODUCTION

A MANET is a collection of mobile nodes that can communicate with each other without the use of any fixed infrastructure. Every mobile node in a MANET behaves like a router as well as user, and communication is performed through multi-hop routing. The network topologies can dynamically change due to the mobility of nodes and their ability to participate or withdraw as they wish. Because nodes may arbitrarily participate or detach from a MANET at will, malicious nodes may also easily intrude. Such malicious nodes threaten a MANET's security through a wide variety of attacks (e.g. viruses, spoofing, route disruption or discarding data). The problem can also spawn from any node to other node for any number of reasons such as mobility issues, resource consumption, or simply from signal interference and collision. Therefore to secure the entire network the authentication mechanisms, intrusion detection systems and encryption technique is used. During festival or disaster, it is nearly impossible to communicate through any fixed infrastructure in terms of deployment cost and difficulty. But MANETs can be deployed quite easily and efficiently in such places. The integration of MANET and other infrastructured networks, e.g. cellular network, WLAN, and internet can expand the coverage area of network and offer some services which are not provided by MANET. For example, integration of MANET and cellular network can widen network coverage area. Another example is the integration of MANET and IP access network which can offer internet access to MANET users whereas they are mobile. To integrate two or more different networks, some aspects, such as gateway selection, efficient routing protocol, handoff management, service discovery, location, connection, and security management are considerably required. The gateway selection is one major aspect to connect MANET and infrastructured network. Various types of heterogeneous network architecture have been proposed. In those architectures, there are many scenarios of gateway discovery, especially in integration of two or three systems, for example cellular network and WLAN, MANET and internet. Although there are many integration schemes, most of them do not discuss about multiple parameters in gateway selection mechanism. During the coupling of a MANET and the Internet, a gateway is placed between the two networks that have direct access to both of them. It can assist with security management in the heterogeneous environment; however, we should note that such a secure gateway should be under the trusted control of a network administrator. While such gateway management can be expensive, multiple gateways or even third party access points (APs) may be deployed in a MANET along with its growth in size. This should make it quite complicated or even impossible to securely manage all the gateways and APs in a MANET. In this paper, we focus on gateway selection mechanism as an essential component to interconnect MANET and infrastructured networks. The continuation of MANET connected with the infrastructured network depends on the appropriate gateway selection. We regard multiple metrics as consideration to select the best gateway. Node remaining energy and gateway load are the metrics to compare. The remaining energy and gateway load metric of gateway represents interconnection lifetime. To calculate these metrics, we use one of Multi-Criteria Decision Making (MCDM) techniques called Simple Additive Weighting (SAW) method. We evaluate throughput performance, Packet Delivery Ratio (PDR) and end-to-end Delay to show the optimization of network performance.

2. INTERNET CONNECTIVITY AND THE ROUTING PROTOCOL

Internet connectivity is an active area in MANET research. One example of early work on the subject is C. Perkins's [1] proposed combination of routing by Ad hoc On-demand Distance Vector (AODV) [2] and mobility management by Mobile Internet Protocol (IP) [3]. Also many architectures and systems have been recently proposed for Internet connectivity. In [4], the operations of the most well-known approaches are compared through logical discussions and simulations. Furthermore, the influence of gateway discovery mechanisms and MANET routing protocols to the performance of those approaches was clearly specified as well. An optimum mechanism is used to select appropriate gateway based on multiple node metrics, such as remaining energy [5] and gateway load [6] for interconnected Mobile Ad Hoc Network (MANET) with infrastructured network [7]. This work will greatly help to design such hybrid MANET architectures in the future. Interconnection between MANETs and the Internet brings much promise, such as the ability to extend an AP's coverage and the realization of ubiquitous computing in society. The interconnection between MANETs and the Internet will require further logical and technical development in many areas including gateway and AP management, mobility management, addressing, routing, etc. The routing protocols are closely related to Internet connectivity and are one of the biggest issues in this field. While there has been much research on MANET routing protocols for Internet connectivity, research on DYMO has mostly been conducted concerning multipath routing and secure routing.

3. PROPOSED METHOD

The DYMO Internet-Draft defines that one or more gateways are necessary for Internet connectivity. We assume that the special sensitive data are handled on these multi-gateway MANETs. Our DYMO routing algorithm directs the special data to a specific secure gateway, while conventional DYMO route discovery does not. First, we classify application data into two types, Special data (s-Data) which includes important, sensitive or advanced information that requires particular security considerations, and normal-data (n-Data) which has no such requirements. While n-Data can be forwarded by any gateway, s-Data must be forwarded by only special gateways (s-GW), which are operated by a trusted network administrator. Based on these assumptions, our proposal uses two types of routes, namely routes for n-Data (n-Route) and routes for s-Data (s-Route). For this purpose, we also classify Routing Messages (RMs), gateway and routing entries according to these data types.

A. Routing Message

The data type is reflected in the Type of Service (ToS) field in the IP header. Every node can determine the data type by its ToS field. When a source node wants to send s-Data, it begins s-Route discovery with a special-RREQ (s-RREQ). The RREP for the s-RREQ also must be a special-RREP (s-RREP), while normal-RREP (n-RREP) is the response to the normal-RREQ (n-RREQ). The type of Routing Messages is determined by the S flag in the message header. The 8-bit field between msg-type and msg-size is called msg-semantics, and describes the interpretation of the rest of the message header. These bits define whether the message header contains an msg-version, originator address, sequence number, or hop count, etc. The most significant bit for our purposes is the R-bit, which means reserved and has no use in the entire MANET specification. Hence, we apply this reserved bit to the S-flag bit. When S is 0, the message is n-RREQ or n-RREP, and when S is 1, the message is s-RREQ or s-RREP. Each MANET node checks the S-bit in the received RM to recognize its type.

B. Gateway Selection

The GW is assumed to know all the MANET node's IP addresses beforehand. When a MANET node tries to discover the route to a destination on the Internet, it broadcasts RREQ as well as the normal route discovery process. The GW can then judge if the destination of the received RREQ is outside the MANET. Once it has the route to the destination on the Internet, it finally initiates RREP for the source node as true destination.

i. if (RREQ message) then
ii. if (status=MANET node) then
iii. send n-Route reply or s-Route reply unicast message
iv. endif
v. else
vi. if (status=GATEWAY node) then
vii. if (it is s-Route request) then
viii. if (status=s-GATEWAY node) then
ix. send s-Route reply unicast message with metric information
x. endif
xi. else
xii. do nothing
xiii. endif
xiv. else
xv. send n-Route reply unicast message with metric information
xvi. else
xvii. if (reply message) then
xviii. if (initial node=node address)
xix. call Gateway selection procedure
xx. else
xxi. send reply unicast message
xxii. endif
xxiii. endif

[*Algorithm of Gateway Selection*]

We define a trusted gateway as an s-GW, which can forward both n-Data and s-Data. A GW that is only trusted to forward n-Data is called an n-GW. Both types of GWs respond to n RREQ with n-RREP. However, n-GWs do not respond to s-RREQ, therefore only s-GWs return s-RREP. To select the gateway, the source node should calculate the multiple metric of each gateway node. Simple Additive weighting (SAW) as one of Multi-Criteria Decision Making (MCDM) method is used to calculate the metric. SAW basically calculates the overall score of a metric as the weighted sum of all metric value. Each metric has different range and different value unit, so firstly have to scale the metrics to bring all metric values into non-dimensional values. The scaling method has two types: positive criteria and negative criteria. Remaining energy metric is calculated with positive criteria and can be calculated from the energy consumption behavior in the ad hoc network node wireless interface. There are various types of energy consumption that have been identified. Energy consumed while sending a packet. Energy consumed while receiving a packet. Energy consumed while in idle mode. Energy consumed while in sleep mode which occurs when the wireless interface of the mobile node is turned off. It should be noted that the energy consumed during sending a packet is the largest source of energy consumption of all modes. Gateway load is calculated with negative criteria. Two types of load are calculated in MANET traffic. They are Inter-MANET traffic load and Intra-MANET traffic load. The Inter-MANET traffic load via each IGW is the number of registered (both local and visiting) MANET nodes sending/receiving traffic to/from Internet via that IGW. The Intra-MANET traffic load is the number of nodes managed by each IGW in the network topology. When the message is received by the neighboring node

4. PERFORMANCE EVALUATION

We used the simulator NS – 2.28 to implement our proposed protocol by modifying DYMO. We have different types of experiments to evaluate the performance of a hybrid MANET and to check whether the proposed GW selection performs the expected routing operations. We initially describe the common settings throughout the entire experiment. Thereafter we introduce experiments and their results.

4.1 Simulation setup

Throughout the simulations the number of MNs deployed in MANET (NMN) is fixed to 15 and the number of GWs deployed in MANET (NGW) is 5. By default, the wired link delay between the destination and each GW (dlink) is 10 ms. The MNs move based on the Random Waypoint Mobility Model. We use a Constant Bit Rate (CBR) for transferring n-Data and s-Data. By default, there is no other traffic. We change the total number of flows (Nflow) 4 to 5 in each experiment.

4.2 Experiments and results

The configuration parameters used for the experiment are shown in Table 1.

Table 1 Simulation environment parameters

Parameter	Value
Simulation time	10 min
Dimension	1,200 m × 1,200 m
NGW	5
NMN	15
MN placement	Random
Mobility model	Random waypoint
Min. speed	0 m/s
Max. speed	3 m/s
Pause time	2 min
I/O queue size	250 kbyte
N flow	4
CBR data size	512 byte
Comm. period	2–7 min
Sending rate	10 packet/s

4.2.1 Delivery ratio and Delay

In this part, experiments are performed to evaluate the delivery ratio, end-to-end delay and energy depletion rate. Figure 1 show that the average Packet Transmission Delay of data packet from IGW to the mobile nodes.

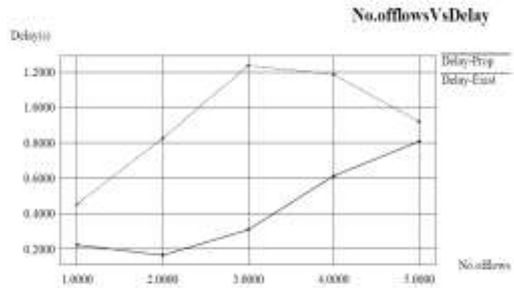

Figure 1: Packet Transmission Delay

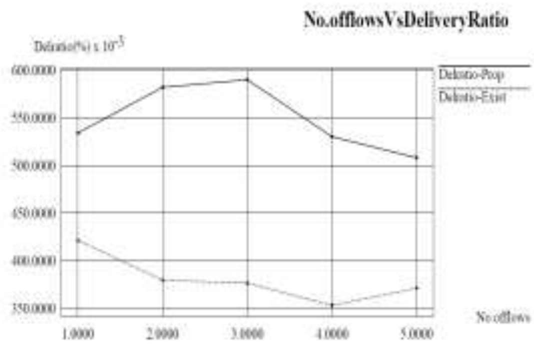

Figure 2: Packet Delivery Ratio

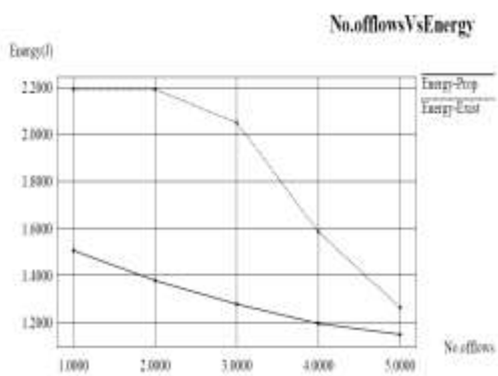

Figure 3: Energy Depletion Rate

When the network load increases, that means due to congestion the delay also increases. However there is a smaller delay if the number of gateways increases because each source node averagely can have less hop count to a gateway. Still it is showing better performance in the DYMO. The figure 2 shows the Packet Delivery Ratio. This is also improved as normal gateway becomes larger, having fewer packets dropped, because the traffics are distributed and traffic has smaller hop. Figure 3 shows the energy depletion rate of the gateways. In the existing system the energy of the gateway is reduced rapidly and the gateway is depleted sooner. But in the proposed system, as it is giving priority to the remaining energy, so the gateways depleted steadily and consequently the average gateway lifetime drops off. Longer gateway lifetime indicates longer network interconnection.

5. CONCLUSION AND FUTURE WORK

Internet connectivity for MANETs is quite attractive in terms of increased variety in communication, and network expansion and accessibility. The proposed routing protocol allows source nodes to forward special sensitive data to the Internet through especially secure/trusted gateways. This ensures that advanced and important data are handled securely by a gateway that is under the trusted control of a network administrator. The proposal is implemented through the modification of DYMO. Conventional DYMO is agnostic to the character of data and trustworthiness of gateways, and instead uses only hop count as a metric for the route discovery process. But the proposed one uses an optimum multiple metrics gateway selection mechanism in the integration of MANET and infrastructured network. SAW calculation uses the MCDM technique. It considers two metrics as selection comparison: remaining energy and gateway load. Simulation results show that the proposed scheme enhance performance of throughput, Packet Delivery Ratio (PDR), Delay and Energy Depletion Rate.

REFERENCES

[1]. Y. Sun, E.M. Belding-Royer and C.E. Perkins, “Internet connectivity for ad hoc mobile networks,” International Journal of Wireless Information Networks, vol. 9 no. 2, pp. 75-88, Apr. 2002.

[2]. C. E. Perkins, E. M. Belding-Royer, and S. R. Das, “Ad hoc on-demand distance vector (AODV) routing,” RFC 3561, Jul. 2003.

[3]. C. E. Perkins, “IP mobility support for IPv4,” RFC 3344, Aug. 2002.

[4]. P.M. Ruiz, F.J. Ros and A. Gomez-Skarmeta, “Internet connectivity for mobile ad hoc networks: Solutions and challenges,” IEEE Communication Magazine, vol. 43, no. 10, pp. 118–125, Oct 2005.

[5]. K. Arulanandam and B. Parthasarathy, “A new energy level efficiency issues in mobile ad hoc network,” International Journal of Reviews in Computing, pp. 67-78, 2009.

[6]. Q. L. Trung, P. E. Engelstad, T. Skeie and A. Taherkordi, “Load-balance of intra/inter-MANET traffic over multiple internet gateways,” Proceedings of the International Conference on Advances in Mobile Computing and Multimedia, Linz, Austria, pages 50-57, November 2008.

[7]. F. P. Setiawan, S. H. Bouk and I. Sasase, “An optimum multiple metrics gateway selection mechanism in MANET and infrastructured networks integration,” Proceedings of IEEE wireless communications networking and mobile computing, pp. 2229-2234, 2008.