Mobile Netw Appl (2010) 15:205–215
DOI 10.1007/s11036-009-0173-6

Gateway Selection Protocol in Hybrid MANET Using DYMO Routing

Takeshi Matsuda · Hidehisa Nakayama · Xuemin (Sherman) Shen · Yoshiaki Nemoto · Nei Kato

Published online: 26 May 2009
© Springer Science + Business Media, LLC 2009

Abstract In this paper, we propose a novel gateway (GW) selection protocol in hybrid Mobile Ad hoc Networks (MANETs). We focus on the situation that occurs when specialized, sensitive data is 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 GW which is controlled by a trusted network administrator. However, there should be multiple GWs deployed in a MANET, where the cost ineffectiveness makes it difficult for a network administrator to simultaneously manage every GW. Because of the risk of forwarding special data through an unmaintained GW, we propose a routing protocol which allows a source node to have sensitive data forwarded to the Internet through a trusted GW. To achieve this desirable performance, we improve upon one of the newest routing protocols, 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. The results show that our protocol can make MANET source nodes choose GWs for specific data.

Keywords mobile ad hoc network · internet connectivity · gateway selection · dynamic MANET on-demand routing

T. Matsuda (✉) · Y. Nemoto · N. Kato
Graduate School of Information Sciences,
Tohoku University, Aramaki-Aoba 6-3-09, Aoba-ku,
Sendai, 980-8579, Japan
e-mail: george@it.ecei.tohoku.ac.jp

H. Nakayama
Department of Electronics and Intelligent Systems,
Tohoku Institute of Technology, Sendai, Japan

X. Shen
Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Canada

1 Introduction

A MANET is a collection of mobile nodes (MNs) that communicate with each other without the use of any fixed infrastructure. Every MN in the MANET has the role of both the router and the user, in which communication is performed through multi-hop routing. In addition, nodes may arbitrarily participate or withdraw from the MANET, and has no restriction on their mobility. In terms of deployment cost and difficulty, MANETs have efficiency in areas such as campus networks, extension of access point coverage, disaster areas, or a place for casual events like concerts or festivals.

Of all the research on MANETs, researches on hybrid MANETs are one of the most popular topics currently. A hybrid MANET is provided by GWs which connect the MANET to the Internet. This gives us various advanced communication and network scalability, and bolsters ubiquitous environments. Hybrid MANETs contribute more than pure MANETs in a variety of scenes described above. Specifically we consider a post-disaster situation. If an earthquake or other natural disaster took place in a certain area, network infrastructures (e.g., communication links, routers, servers, etc.) could be disabled along with the other infrastructures (e.g., streets, railways). Therefore

the local government and/or the telecommunication carrier should deploy GWs (in ad-hoc manner) to connect MANETs to the Internet through their neighboring networks. In this situation, the role of the hybrid MANET is not only to provide the daily communication (e.g., e-mail, web browsing, telephony) but also to carry essential data (e.g., rescue information and medical records), which will greatly help to relieve disaster victims. In the latter case, the data has major security requirements (e.g., privacy and confidentiality).

However, the MANETs' features described above make it difficult to guarantee security. Malicious nodes could easily intrude, and threaten MANET's security through a wide variety of attacks (e.g., viruses, spoofing, route disruption, eavesdropping, forging or discarding data) [1–3]. In addition, problems can spawn from any node, for any number of reasons, including mobility issues, resource consumption, or simply from signal interference or collision. Therefore, securing the entire network by some security mechanisms (e.g., authentication mechanisms, intrusion detection systems, encryption techniques) are some of the most important issues [4–6]. Although a certain centralized security authority is generally difficult to be deployed in MANETs, GW can assist with security management during the coupling of a MANET and the Internet.

On the other hand, to relay sensitive data, GW also must be under the trusted control of a network administrator. While such GW management can be expensive, MANET should have multiple GWs to keep the quality of communications. This will make it quite complicated or even impossible to securely manage all the GWs. Therefore, there is a trade-off between securing sensitive data and progressing the quality of communications.

In this paper, we intentionally deliver such special data described above to a fully-secure GW, while allowing the existence of GWs with minimal security only for normal data. This can be achieved effectively by enabling the MANET routing protocol to allow selection of GW depending on the sensitivity of data.

In addition, we consider that different types of data are handled in MANET communication. Multiple GWs provide Internet connectivity, and only trusted GWs can be used to forward sensitive data to the Internet. To achieve this, we propose to add additional functionality to the existing MANET routing protocol, DYMO [7]. This modification will allow DYMO to discover routes to appropriate GW depending on the type of application data.[1]

[1]Part of this work has been presented at WiMob'2008 [8].

The remainder of this paper is organized as follows. In Section 2, we first describe the coupling process between a MANET and the Internet, and discuss the significance of the routing protocols to realize such interconnection. Then we discuss the details of the DYMO protocol. Section 3 proposes our routing protocol. In Section 4, initially some experiments on MANET's Internet connection are conducted, and then the performance evaluation of the protocol is evaluated in comparison to conventional DYMO. Finally we draw a conclusion and also refer to the future works in Section 5.

2 Hybrid MANET and MANET routing protocol

2.1 Research on hybrid MANET

Hybrid MANET brings much promise for the realization of ubiquitous computing. Therefore, the Internet connectivity is an active area in MANET research and a significant amount of work has been conducted. One example of early work on the subject is the combination of routing [9] by Ad hoc On-demand Distance Vector (AODV) [10] and mobility management by Mobile Internet Protocol (IP) [11]. Additionally, many architectures and systems have been recently proposed for Internet connectivity. In [12], the operations of the most well-known approaches are compared through logical discussions and simulations. Furthermore, the influence of GW discovery mechanisms and MANET routing protocols to the performance of those approaches are clearly specified, which can greatly help to design such hybrid MANET architectures in the future.

Hybrid MANETs have many differences from pure MANETs, and much research has been done in this area, such as GW management, mobility management, addressing, and routing. Robust interconnection between MANETs and the Internet will require further logical and technical development in these areas. Of all the topics related to hybrid MANETs, GW discovery has been actively researched [13, 14]. Most research focuses on hop count, GW's load condition, and node mobility as a GW selection metric. However, none of them consider data character as a metric.

2.2 MANET routing protocols

Routing protocols are one of the main challenges in MANETs. A good number of researches on MANET routing have been proposed, and most of them can be largely categorized into Reactive and Proactive approaches.

The reactive protocols, such as AODV and Dynamic Source Routing (DSR) [15], enable on-demand route discovery and offer low processing, memory overhead, and network utilization. In contrast, proactive protocols such as Optimized Link State Routing (OLSR) [16] and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [17], enable every node to comprehend the entire network topology and to initiate a connection quickly according to periodic information exchange.

Currently the Working Group (WG) of the Internet Engineering Task Force (IETF) is conducting research regarding practical MANET use [18], including developing a unified packet format [19] and working towards a standardization of routing protocols. DYMO is one of their perspective protocols and grabs attention as the future representative of reactive routing protocols.

2.3 DYMO routing

DYMO is the successor of AODV, but there are many remarkable changes such as a unified packet format, a simplified RERR algorithm, and multiple interface utilization. Furthermore, the Internet connectivity is also defined in the DYMO Internet-Draft [7], and is the most attractive specification yet towards practical MANET use. In the following, we will outline the core routing and Internet connection algorithms of DYMO.

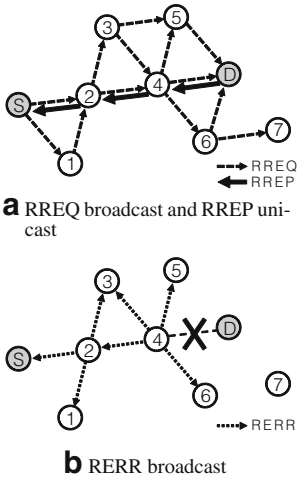
As DYMO is a type of reactive routing protocol, it consists of two operations: route discovery and route maintenance.

2.3.1 Route discovery and route maintenance

The route discovery begins with the flooding of Route Request (RREQ) messages by a source node. As shown in Fig. 1a, RREQ is broadcast from source S, received by the neighbor nodes of S, and then is re-broadcast. This multihop transmission allows the RREQ to reach the expected destination D. In response to the RREQ, D unicasts Route Reply (RREP) messages toward S. This RREP will eventually reach the source node through the multihop path. In this way, the route from S to D is established. It should be noted that this path is the shortest path out among possible routes, and is loop-free. The intermediate nodes which forwarded both the RREQ and RREP messages take the role of routers. The route S–2–4–D is established in Fig. 1a.

Because each node serves as a router, those currently involved in some data transmission maintain their own routing table which consists of a destination IP, next hop IP, sequence number, route timeout, and also the information regarding whether the destination is GW or not. Multiple entries for the same destination in a routing table cannot exist. When nodes receive or successfully send a message, they update the information in the routing entry according to the message. In this way, every active route is kept fresh, loop-free, and the shortest.

Fig. 1 **a**, **b** DYMO route discovery and maintenance



a RREQ broadcast and RREP unicast

b RERR broadcast

When an intermediate node finds a broken link, or when it receives a datagram and does not know where to forward it, it broadcasts a Route Error (RERR) message with the information about the unreachable destination. The RERR messages are forwarded by intermediate nodes until the message reaches the source node of the broken route or the no-route datagram. In Fig. 1b, node 4 finds the link to D has been broken and broadcasts a RERR. The RERR is sent to S through the intermediate node 2.

2.3.2 Internet connectivity

In addition to the above routing operations, Internet connectivity is also defined in the DYMO Internet-Draft. The existence of a GW (called Internet DYMO Router (IDR) in the draft) is essential in establishing a connection to the Internet. The GW is assumed to know all the MANET nodes' 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 described above. 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 on behalf of the true destination.

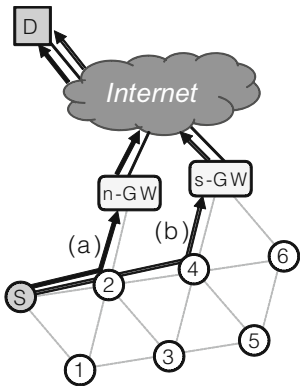


Fig. 2 Data transmission to the Internet

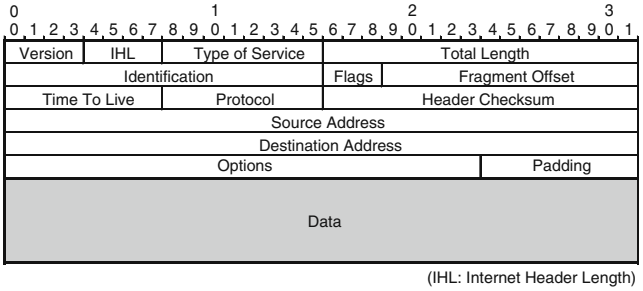


Fig. 3 Data packet format

Additionally, the DYMO Internet-Draft also allows for multiple GWs in a MANET, which is convenient when the size of a MANET is too large to be covered by a GW. In the topology of Fig. 2, both of the two GWs receive the RREQ from source S, and return RREP to S. As a result, S receives two different RREPs of the same destination. According to the DYMO algorithm, nodes prefer the minimal hop route, so only route (a) is used for data transmission to D.

While there has been much research done on MANET routing for Internet connectivity, research on DYMO has mostly been conducted concerning multipath routing [20], secure routing [21], and some performance comparison among MANET routing protocols [22]. There exists only one research concerning the MANET-Internet connection, which studied the DYMO performance in Vehicular Ad hoc Network (VANET) environment [23].

3 Proposed gateway selection routing

The DYMO Internet-Draft defines that one or more GWs are necessary for Internet connectivity. We assume that the special sensitive data are handled by these hybrid MANETs with multiple GWs. Our DYMO routing algorithm directs the special data to a specific secure GW, while conventional DYMO route discovery does not.

3.1 Data type definition

First, we classify application data into two types. The value of the data type should be determined by a network administrator beforehand. Conceptually, only sensitive data such as rescue information and medical record should be treated as the special-Data (s-Data), and the others such as e-mail and web browsing should be the normal-Data (n-Data). Recognizing this classification can easily be achieved just by checking the software or application that generates data packets (e.g., web browser or an application dedicated to rescue activity).

As s-Data requires particular security considerations, they must be forwarded by only Special-Gateways (s-GW), which are operated by a trusted network administrator. And as n-Data has no such requirements, they can be forwarded by Normal-Gateways (n-GWs).

Technically, DYMO cannot refer to application data directly. We need to reflect data-types into Type of Service (ToS) field [24] in IP header. Figure 3 shows the generic IP header format. ToS[2] field is the second octet in it. This field is intended to denote the importance or priority of the datagram, or other communication specialty. This data type reflection also enables DYMO to know the type of data.

Based on these assumptions, our protocol 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), GW and routing entries according to these data types.

3.2 Routing message

When a source node wants to send s-Data to a destination without any pre-established route, 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).

Figure 4 shows the overview of DYMO RREQ packet, which follows the unified MANET packet format [19]. The type of a RM (RREQ, RREP, or RERR) is determined by msg-type field in Message Header. To determine RM specialty (i.e. n-RREQ or s-RREQ, and

[2]According to the latest RFCs, the first six bits are assigned as Differentiated Services (DS) Field [25], and the last two bits are called Explicit Congestion Notification (ECN) field [26].

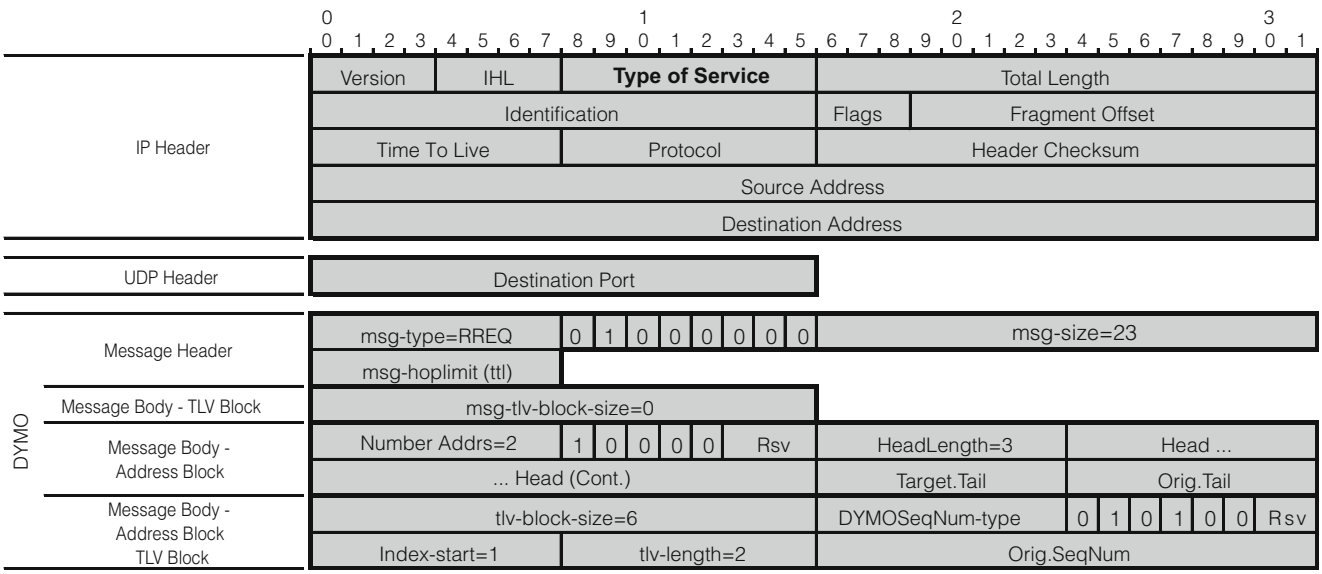


Fig. 4 DYMO packet format (RREQ)

n-RREP or s-RREP), we assign the S-flag to one bit in ToS field, as well as the data type determination in Section 3.1. If S-flag is cleared (0), the message is either n-RREQ or n-RREP, and if set (1), the message is either s-RREQ or s-RREP. Each MANET node checks the S-flag in the received RM to recognize its type.

3.3 Gateway

We define a trusted gateway as a s-GW, which can forward both n-Data and s-Data. A GW that is only trusted to forward n-Data is called a n-GW. Figure 5 depicts the RREQ reception algorithm which represents the difference between a n-GW and a s-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. In this way, the source node that sends an s-Data can limit the relaying gateways to s-GWs.

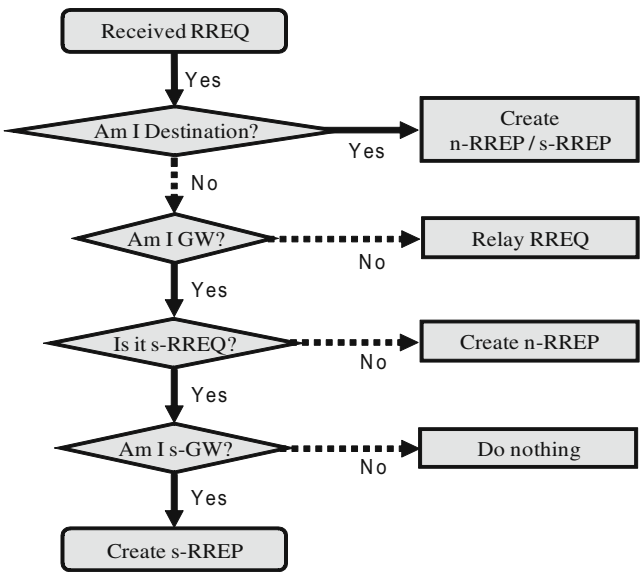


Fig. 5 Algorithm of the response to received RREQ

We explain how the proposed routing protocol affects route discovery for s-Data in Fig. 2. With our proposed routing method, the s-Data owned by node S must be transmitted through route (b), even though there is a shorter route (a) which would normally be selected by the DYMO algorithm. Thus, our protocol considers both of the data-type and the GW, as well as the hop count.

3.4 Routing entry

To achieve the desired routing behavior, we must also modify routing entries by attaching S-flag. S-flag can be used to identify the type of routing entry: entries with $S = 0$ are for n-Data, while those with $S = 1$ are for s-Data. Therefore, a MANET node can have two routing entries which have the same destination but different

Table 1 Example of the routing table of node 2 in Fig. 2

Destination	Sequence number	Hop count	Next hop	S
S	...	1	S	0
S	...	1	S	1
D	...	1	n-GW	0
D	...	2	4	1
...	...	...	...	...

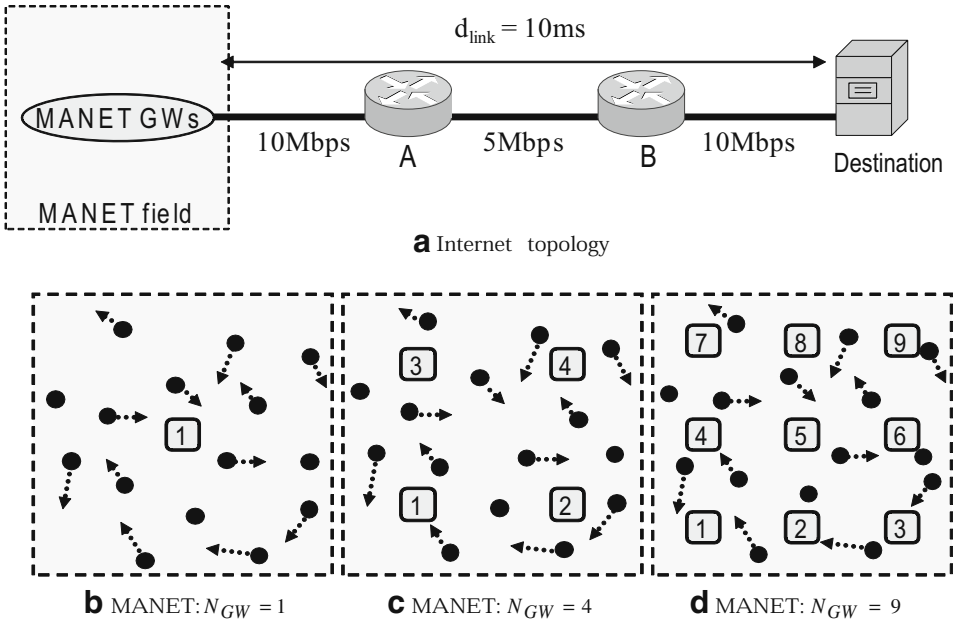


Fig. 6 **a–d** Simulation topology

S value as shown in Table 1. Traditional DYMO only allows one entry per destination.

4 Performance evaluation

We used the commercial simulator QualNet 4.0 (Scalable Network Technologies, Qualnet, http://www.scalable-networks.com/) to implement our proposed protocol by modifying DYMO which is preinstalled. 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 two experiments and their results, where the additional settings for each experiment are individually denoted.

Table 2 Simulation environment

Parameter	Value
Simulation time	10 min
Number of executions	50
Dimension	1,800 m × 1,800 m
N_{GW}	1, 4, 9
N_{MN}	100
MN placement	Random
Mobility model	Random waypoint
Min. speed	0 m/s
Max. speed	3 m/s
Pause time	2 min
Input/output queue size	50 kbyte
N_{flow}	1–10
CBR data size	512 byte
Communication period	2–7 min
Sending rate	10 packet/s

4.1 Simulation setup

Throughout all simulations, while the number of MNs deployed in MANET (N_{MN}) is fixed to 100, the number of GWs deployed in MANET (N_{GW}) is 1, 4, or 9, so GWs are deployed uniformly as shown in Fig. 6b, c, or d. Figure 6a depicts that every GW is connected to the destination through the router A, and the bottleneck link (between router A and B) bandwidth is 5 Mbps. By default, the wired link delay between the destination and each GW (d_{link}) is 10 ms. The MNs move based on the Random Waypoint Mobility Model [27].

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 (N_{flow}) from 1 to 10 in each experiment.

Each experiment conducts the simulation 50 times, each with different random value seeds. Therefore, each of the following results are an average of repetition.

We also have other configurations in Tables 2 and 3.

Table 3 DYMO configuration

Parameter	Value
Net diameter	10
Traversal time	0.040 s
Valid route timeout	5 s
Delete route timeout	25 s
RREQ retries	3

4.2 Experiments and results

4.2.1 Exp.1: delivery ratio and end-to-end delay

In this part, experiments are performed to evaluate the delivery ratio and end-to-end delay. Simulations are performed with different number of GWs.

Figure 7a shows the average end-to-end delay of each experiment. In all simulations, the end-to-end delay is larger than the configured d_{link} (=10 ms), and due to the congestion, it becomes larger as the traffic increase in MANET. However, we had smaller delays as the number of GWs increases because each source node averagely can have less hop count to a GW.

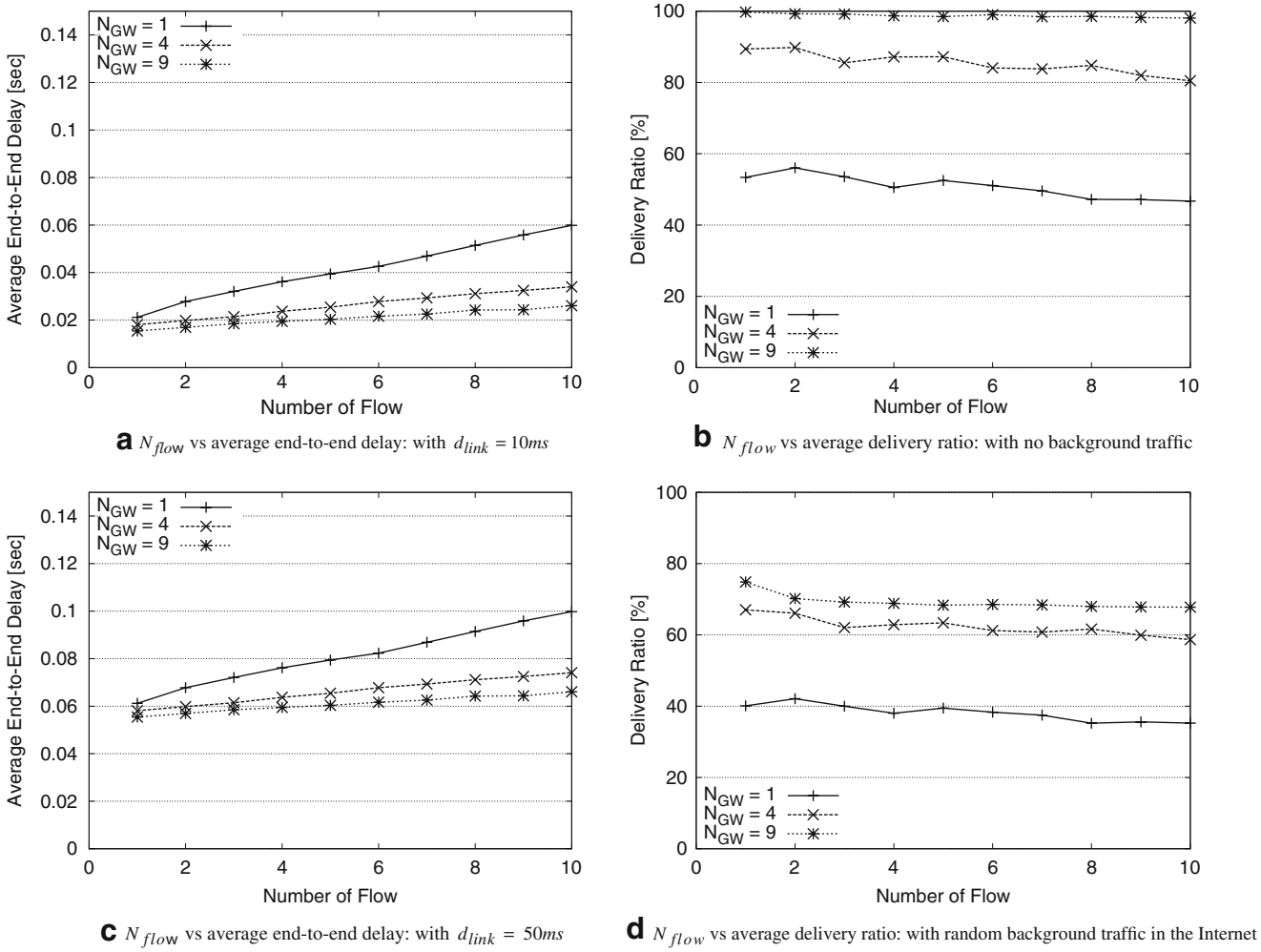
Figure 7b shows the delivery ratio of each experiment. This is also improved as N_{GW} becomes larger, having fewer packets dropped, because the traffics are distributed and each traffic has smaller hop.

Additionally, we simulated the scenarios where $d_{\text{link}} = 50$ ms. Figure 7c shows the average end-to-end delay in these scenarios. All simulations had larger delay than the configured $d_{\text{link}} (= 50$ ms) . In comparison with Fig. 7a, we can say the link delay in the wired environment equally affects all traffic.

Furthermore, we also simulated the scenarios concerning random background traffic in wired environment, whose data size and interval are random along with the exponential distribution, and consumes bandwidth in a random manner. Its average data size is 2,048 bytes, and average interval is 1 ms.

Figure 7d shows the delivery ratio in these scenarios. In comparison with the results in Fig. 7b, the number of received packets is about 30% smaller in all simulations. This is because, in all simulations, the data traffic from MANET has almost equal possibility of packet drop due to the background traffic.

Figure 8 depicts how much the number of received packets has changed in each simulation because of the background traffic. We also have to note that all GWs are connected to the same router A in Fig. 6a. Due



a N_{flow} vs average end-to-end delay: with $d_{link} = 10ms$

b N_{flow} vs average delivery ratio: with no background traffic

c N_{flow} vs average end-to-end delay: with $d_{link} = 50ms$

d N_{flow} vs average delivery ratio: with random background traffic in the Internet

Fig. 7 **a–d** Exp.1: end-to-end and delivery ratio

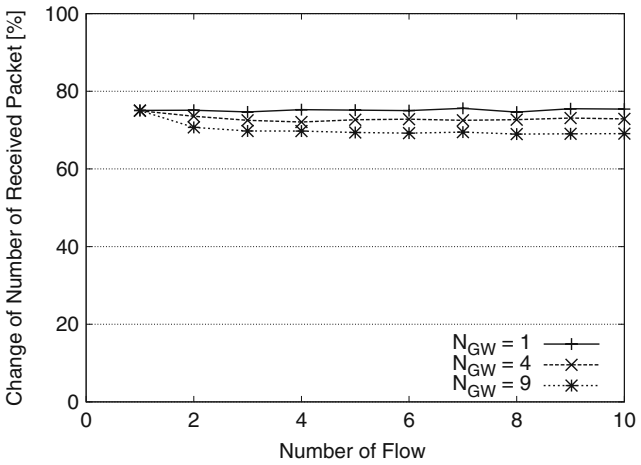


Fig. 8 Degradation of number of received packet: comparison between the experiment with background traffic and the one without

to this topology, the more GWs there are, the more packets are handled in parallel, which makes data traffic density higher on router A. As a result, when there are more GWs, we have more packet drop on the Internet although traffic is well distributed within MANET.

4.2.2 Exp.2: GW behavior

In this part, we introduce the experiments evaluating performance of our proposal. The number of GWs and the number of source node are fixed to 9 and 10, respectively. Half of the source nodes send s-Data.

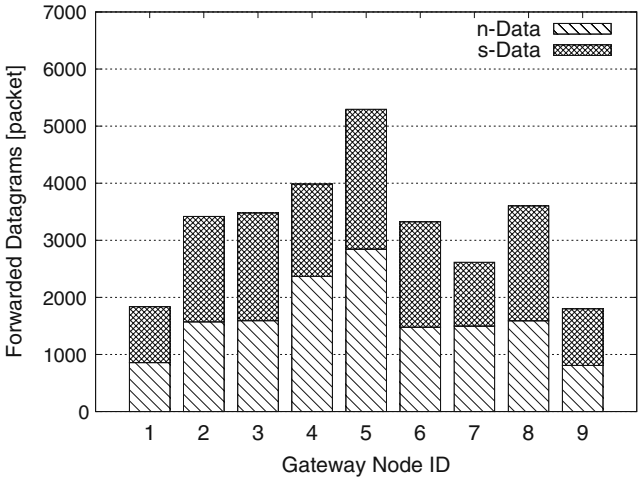
The first experiment (Exp.2-1) is performed with conventional DYMO. These results will be compared with the one in our proposal.

The second experiment (Exp.2-2) is performed with our proposal. GW 1, 3, 7, 9 are s-GWs, and the others are n-GWs in Fig. 6d.

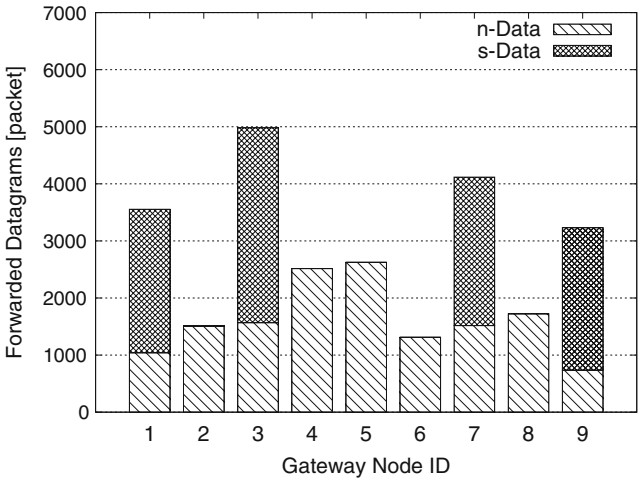
The third experiment (Exp.2-3) is also performed with our proposal. In this experiment, we changed GW assignments: GW 2, 4, 5, 6, 9 are s-GWs, and the others are n-GWs in Fig. 6d. This change is made to demonstrate that the proposed route discovery leads s-Data to an s-GW without relying on their particular location.

Figure 9a–c depict the average number of n-Data and s-Data packets forwarded by the GWs in each experiment.

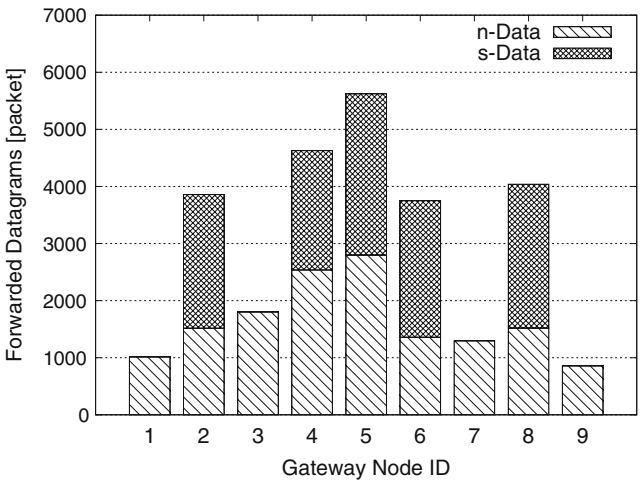
Figure 9a depicts the result of Exp.2-1, which shows that every GW forwards datagrams without any regard of data type. On the other hand, Fig. 9b depicts the result of Exp.2-2, which shows all s-Data is directed



a Exp.2-1: with DYMO



b Exp.2-2: with Proposal (s-GW: 1, 3, 7, 9)



c Exp.2-3: with Proposal (s-GW: 2, 4, 5, 6, 8)

Fig. 9 **a–c** Exp.2: number of forwarded datagrams by GWs

Table 4 Exp.2: total transmission result of datagrams

	Exp.2-1	Exp.2-2	Exp.2-3
Total sent	30,000		
Average received	29,440.6	25,172.3	26,872.4
Average dropped	559.4	4,827.7	3,127.6
Delivery ratio (%)	98.14	83.91	89.57

to only s-GWs. From this figure, we can see that our proposal works correctly.

We can also see the same behavior from the result of Exp.2-3 shown in Fig. 9c. Like Exp.2-2, only s-GWs handle the s-Data. Moreover, the difference between the result of Exp.2-2 and Exp.2-3 indicates that our proposal can select s-GWs wherever they are deployed.

The average packet transmission in each experiment is shown in Table 4. The number of drops for our proposal (Exp.2-2, 2-3) is clearly greater than that of conventional DYMO (Exp.2-1). In our proposal, because all s-Data packets are directed to s-GWs, a traffic imbalance occurs between n-GWs and s-GWs. As a result, s-GW and MNs around the s-GW lose packets due to signal collision, interference, and queue overflow. Additionally, the number of drops in Exp.2-3 is less than that of Exp.2-2 because Exp.2-3 has more s-GWs.

5 Conclusion and future work

We proposed a routing protocol which allows source nodes to forward special sensitive data to the Internet through especially secure/trusted GWs. This ensures that advanced and important data are handled securely by a GW that is under the control of a trusted network administrator.

Our protocol is implemented through the modification of DYMO. Conventional DYMO is agnostic to the character of data and trustworthiness of GWs, and only uses hop count as a metric for the route discovery process. To include the character of data and GWs into the DYMO routing metrics, we have classified data into sensitive and normal data. The routing messages, GWs and routing entries are also classified into n-Routes and s-Routes so that the routes are individually established according to the data-type and destination.

Simulation results show that packet delivery ratio and end-to-end delay are improved as the number of GW deployed increases, and that our protocol correctly selects the s-GW for transmission of the s-Data. However, this comes at a cost of increased packet drop.

To mitigate traffic concentration on s-GWs and the MNs around them, implementation of an appropriate load balancing mechanism should be examined in future works. One study is found in [14], which considers congestion level as an additional metric for GW selection, as well as hop count. GWs periodically send their advertisement messages which include load congestion information of themselves and around them.

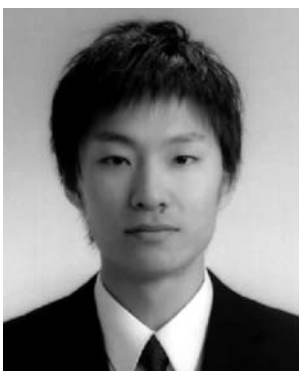
Actually, our original proposed method was intended to use the reserved bit in DYMO message header as S-flag. However, because of the current frequent updates of DYMO Internet-Draft, wether the S-flag can be guaranteed in the DYMO message header is still with uncertainty. There is still a long way to go even before DYMO reaches the stage of implementation. We believe that the S-flag can be considered as one of the DYMO options in the future.

Acknowledgements This work was supported through the International Communications Research Grant (A Study on Reliable Ad hoc Networks, 2009), International Communications Foundation (ICF).

References

1. Hu Y-C, Perrig A, Johnson D (2003) Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proc of the 2003 ACM workshop on wireless security (WiSe '03), pp 30–40
2. Hu Y-C, Perrig A, Johnson D (2006) Wormhole attacks in wireless networks. IEEE J Sel Areas Commun 24(2):370–380
3. Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A (2007) A survey of routing attacks in mobile ad hoc networks. IEEE Wirel Commun Mag 14(5):85–91
4. Sanzgiri K, LaFlamme D, Dahill B, Levine BN, Shields C, Belding-Royer EM (2005) Authenticated routing for ad hoc networks. IEEE J Sel Areas Commun 23(3):598–610
5. Zhou L, Haas Z (1999) Securing ad hoc networks. IEEE Netw 13(6):24–30
6. Papadimitratos P, Haas Z (2003) Secure data transmission in mobile ad hoc networks. In: Proc of the 2003 ACM workshop on wireless security (WiSE '03), pp 41–50
7. Chakeres I, Perkins C (2008) Dynamic MANET on-demand (DYMO) routing. IETF Internet-Draft, draft-ietf-manet-dymo-16
8. Matsuda T, Nakayama H, Shen S, Nemoto Y, Kato N (2008) On gateway selection protocol for DYMO-based MANET. In: Proc 4th IEEE int conf on wireless and mobile computing, networking and communications (WIMOB'08), Avignon, France, pp 32–37
9. Sun Y, Belding-Royer EM, Perkins CE (2002) Internet connectivity for ad hoc mobile networks. Int J Wirel Inf Netw 9(2):75–88
10. Perkins CE, Belding-Royer EM, Das SR (2003) Ad hoc on-demand distance vector (AODV) routing. RFC3561
11. Perkins C (2002) IP mobility support for IPv4. RFC3344
12. Ruiz PM, Ros FJ, Gomez-Skarmeta A (2005) Internet connectivity for mobile ad hoc networks: solutions and challenges. IEEE Wirel Commun Mag 43(10):118–125
13. Ghassemian M, Hofmann P, Prehofer C, Friderikos V, Aghvami H (2004) Performance analysis of internet gateway

discovery protocols in ad hoc networks. In: Wireless communications and networking conference, 2004 WCNC, vol 1. IEEE, pp 120–125
14. Rakesh K, Manoj M, Sarje AK (2007) An efficient gateway discovery in ad hoc networks for internet connectivity. In: Proc of computational intelligence and multimedia applications, pp 275–282
15. Johnson D, Hu Y-C, Maltz D (2007) The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. RFC4728
16. Clausen ET, Jacquet EP (2003) Optimized link state routing protocol (OLSR). RFC3626
17. Ogier R, Templin F, Lewis M (2004) Topology dissemination based on reverse-path forwarding (TBRPF). RFC3684
18. Chakeres ID, Macker JP (2007) Mobile ad hoc networking and the IETF. ACM SIGMOBILE Mob Comput Commun Rev 11(4):80–82
19. Clausen T, Dearlove C, Dean J, Adjih C (2008) Generalized manet packet/message format. IETF Internet-Draft, draft-ietf-manet-packetbb-17
20. Galvez JJ, Ruiz PM (2007) Design and performance evaluation of multipath extensions for the DYMO protocol. In: Proc of the 32nd IEEE conference on local computer networks (LCN '07). IEEE Computer Society, Washington, DC, USA, pp 885–892
21. Rifa-Pous H, Herrera-Joancomarti J (2007) Secure dynamic MANET on-demand (SEDYMO) routing protocol. In: Proc of the fifth annual conference on communication networks and services research (CNSR), pp 372–380
22. Johnson D, Lysko A (2008) Comparison of MANET routing protocols using a scaled indoor wireless grid. Mob Netw Appl 13(1–2):82–96
23. Sommer C, Dressier F (2007) The DYMO routing protocol in VANET scenarios. In: Vehicular technology conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, 30 2007-3 October 2007, pp 16–20
24. Almquist P (1992) Type of service in the internet protocol suite. RFC1349
25. Nichols K, Blake S, Baker F, Black D (1998) Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers. RFC2474
26. Ramakrishnan K, Floyd S, Black D (2001) The addition of explicit congestion notification (ecn) to ip. RFC3168
27. Bettstetter C, Resta G, Santi P (2003) The node distribution of the random waypoint mobility model for wireless ad hoc networks. IEEE Trans Mob Comput 2(3):257–269



Takeshi Matsuda received his B.E degree from the Group of Communication Engineering, School of Engineering at Tohoku University in March 2008. Currently, he is working toward an M.S. degree at the Graduate School of Information Science (GSIS), Tohoku University. His research interests are in the area of ad hoc networking, specifically routing. He is the recipient of the student best paper award at the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2008).

Hidehisa Nakayama received his B.E., M.S. and Ph.D. degrees in Information Sciences from Tohoku University in 2000, 2002, and 2005, respectively. He is a senior assistant professor and currently working for Tohoku Institute of Technology. He has been engaged in research on intelligent sensor technology, wireless mobile ad hoc network, computer networking, character string analysis, pattern recognition, and image processing. He is a member of IEEE Communications Society, the Institute of Electronics, Information and Communication Engineers (IEICE), and the Information Processing Society of Japan (IPSJ). He received the Paper Award for Young Researcher of IPSJ Tohoku Chapter in 2000 and the Best Paper of Pattern Recognition Award in SCI 2003.

Xuemin (Sherman) Shen (IEEE M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Research Chair Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks.

He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen serves as the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

Yoshiaki Nemoto received his B.E., M.E., and Ph.D. degrees from Tohoku University in 1968, 1979, and 1973, respectively. He was a full professor with the Graduate School of Information Sciences until 2008. Currently he is serving as the senior vice president of Tohoku University. He has been engaged in research work on micro wave networks, communication systems, computer network systems, image processing, and handwritten character recognition. He is a co-recipient of the 1982 Microwave Prize from the IEEE MTT society, the 2005 Distinguished Contributions to Satellite Communications award from IEEE ComSoc society, FUNAI information Science Award 2007 and several prestigious awards from Japanese Ministries. He is a senior member of IEEE, and a fellow member of IEICE and IPSJ.

Nei Kato received his M.S. and Ph.D. Degrees in information engineering from Tohoku University, Japan, in 1988 and 1991, respectively. He joined Computer Center of Tohoku University at 1991, and has been a full professor at the Graduate School of Information Sciences from 2003. He has been engaged in research on computer networking, wireless mobile communications, image processing and neural networks. He has published more than 150 papers in journals and peer-reviewed conference proceedings. Nei Kato has served as a symposium co-chair for GLOBECOM'07 and ChinaCom'08, and TPC member for a large number of IEEE international conferences, including ICC, GLOBECOM, WCNC and HPSR. He is a technical editor of IEEE Wireless Communications from 2006, an editor of IEEE Transactions on Wireless Communications from 2008, a co-guest-editor for IEEE Wireless Communications Magazine SI on "Wireless Communications for E-healthcare". He is a co-recipient of the 2005 Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee, the co-recipient of FUNAI information Science Award, 2007, and the co-recipient of 2008 TELCOM System Technology Award from Foundation for Electrical Communications diffusion. He is serving as an expert member of Telecommunications Council, Ministry of Internal Affairs and Communications, Japan. Nei Kato is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a senior member of IEEE.