東海大学紀要情報通信学部
Vol.11,No.1,2018,pp.7-14

Paper

Ad hoc On-Demand Distance Vector Routing with Reachability Checking as a Countermeasure against Black Hole Attacks

by

Thongcharoen JETTAPHAT [*1] and Junichi MURAYAMA[*2]

(received on Mar.29, 2018 & accepted on Jul.27, 2018)

Abstract

A mobile ad hoc network (MANET) attracts wide attention as a future device network. For achieving high mobility, ad hoc on-demand distance vector (AODV) routing is suitable. However, an AODV-based MANET is vulnerable against a black hole attack. Secure AODV (SAODV) is the conventional countermeasure in order to bypass a black hole. However, it may cause misrouting under the normal conditions. In order to solve this problem, we propose a novel countermeasure scheme. This scheme comprises AODV, reachability checking function and reachability-information caching function. Reachability checking suppresses misrouting effectively. Furthermore, reachability-information caching suppresses control overhead of reachability checking. As the result, our proposed scheme is an attractive countermeasure against black hole attacks.

Keywords: *MANET, AODV, Black hole attack, SAODV, Reachability check, Reachability-information cache*

1. Introduction

A mobile ad hoc network (MANET) attracts wide attention as an Infrastructure-less wireless network [1]. In this network, communication devices behave autonomously for connecting with each other. This feature seems suitable for the base of Internet of things (IoT) [2]. Typical IoT examples are sensor networks, vehicle networks [3] and emergency smartphone networks [4]. Thus, device mobility is its important requirement.

In order to achieve high mobility, ad hoc on-demand distance vector (AODV) routing [5] is suitable. In this routing, control packets are sent on demand and their source addresses are learned at each relay host. Then packets can be forwarded toward the address-learned direction in a hop-by-hop scheme.

However, an AODV-based MANET is vulnerable against a black hole attack [6]. In this attack, a black hole node sends a malicious control packet for absorbing data packets. At the black hole node, the absorbed data packets are discarded. Consequently, communications in a MANET are interfered.

As the conventional countermeasure, Secure AODV (SAODV) [7] has been proposed. It can establish a bypass route using the secondary-received control packet. However, it may not select an appropriate control packet under the normal conditions. Here, the normal condition means that a black hole node is not attacking. Accordingly, data packets are not forwarded along the optimal routes.

In order to solve this problem, we propose a novel countermeasure scheme. In this scheme, we combine AODV routing with a reachability checking function and a reachability-information caching function. Here, we check reachability in order to determine whether an arrived control packet is legitimate or malicious. This check effectively suppresses misrouting in the normal conditions. On the other hand, this check increases control overhead in routing processing. In order to suppress this overhead, we also cache checked reachability-information. This cached information is reused for a short time. Consequently, frequency of checking can be reduced.

Our scheme is evaluated by means of simulation. The result has shown that our scheme is secure and achieves good performance. Consequently, we can say that the proposed scheme is an attractive countermeasure against black hole attacks.

The rest of this paper is organized as follows: Sect. 2 introduces the base technologies as related works and Sect. 3 shows the conventional countermeasure against black hole attacks. Then, Sect. 4 proposes the novel countermeasure and Sect. 5 evaluates the proposed scheme. Next, Sect. 6 discusses applicability of our scheme to multipath conditions. Finally, Sect. 7 concludes this paper with brief summary.

2. Related Works

This section shows the base technologies as related works. We are assuming a network model composed of MANET and AODV. In addition, a black hole attack is assumed as an attack model. They are described in this section.

2.1 *MANET*

MANET is an infrastructure-less wireless network [1]. This network comprises only host devices. They are connected with each other without any access points. For

*1 Graduate School of Information and Telecommunication Engineering, Course of Information and Telecommunication Engineering, Master's Program
*2 School of Information and Telecommunication Engineering, Department of Communication and Network Engineering, Professor

achieving such behavior, they act autonomously. MANET is designed as the base of IoT [2]. Thus, it is assumed to be applied to such as sensor networks, vehicle networks [3] and emergency smartphone networks [4]. From this background, device mobility is an important requirement for MANET.

2.2 *AODV*

In order to achieve high mobility feature, routing is an important issue. A well-known solution is to deploy AODV routing [5]. This routing scheme is based on source-address learning like Ethernet switches.

Fig. 1 shows this mechanism. (1) First, the source host floods a route request (RREQ) packet towards the destination host. (2) Each relaying host learns the source address of the flooding RREQ packet. (3) The destination host that received the RREQ packet returns the route reply (RREP) packet to the source host. This RREP packet is unicasted to the source host hop-by-hop using learned address. Each relaying host also learns the source address of the returned RREP packet.

After this control procedure, the source host can send data packets to the destination host by unicasting way. Likewise, the destination host can also unicast data packets to the source host.

This RREQ packet is sent on demand in order to achieve high mobility feature.

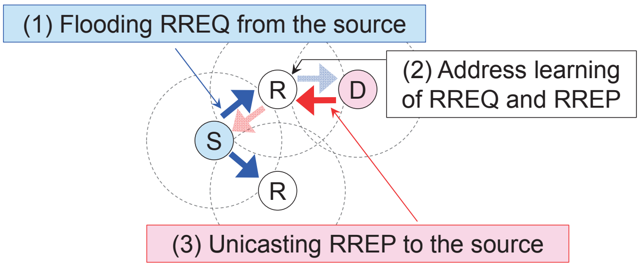
(1) Flooding RREQ from the source
(2) Address learning of RREQ and RREP
(3) Unicasting RREP to the source
R
D
S
R

Fig. 1 Overview of AODV.

2.3 *Black hole attack*

A black hole attack is a well-known attack targeted to an AODV-based MANET [6]. Routing control in both mobile and autonomous environment is vulnerable against such as black hole attacks. This is because specifying malicious control packets under such an environment is not easy.

Fig. 2 shows a mechanism of this attack. (1) First, the source host floods a RREQ packet towards the destination host. (2) A black hole node returns a fake RREP packet when it receives a RREQ packet sent to another hosts. Then, this fake RREP packet is used to establish a fake route towards the black hole node. In many cases, a black hole node may locate nearer than destination hosts. (3) Consequently, this fake route is selected for data packet forwarding. (4) Contrary, the legitimate route is ignored despite that the legitimate RREP packet is arrived. This is due to their arrival order.

After those procedures, data packets are forwarded along the fake route. Then, they are simply discarded at the black hole node. Consequently, communications in a MANET are interfered.

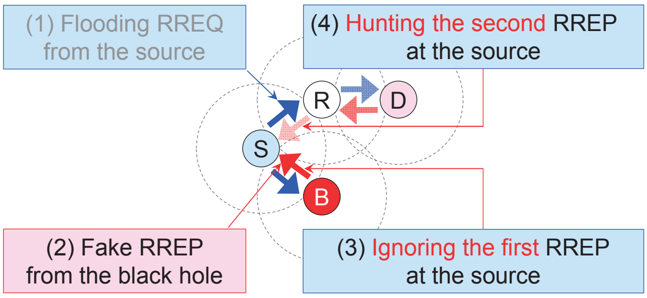
(1) Flooding RREQ from the source
(4) Hunting the second RREP at the source
R
D
S
B
(2) Fake RREP from the black hole
(3) Ignoring the first RREP at the source

Fig. 2 Overview of a black hole attack.

3. Conventional Countermeasure

SAODV [7] is the conventional countermeasure against black hole attacks. This scheme is a kind of modified AODV. It pays attention to the order of arrival RREP packets. In many cases, a fake RREP packet arrives faster than a legitimate RREP packet. Here, the original AODV uses only the first-arrived RREP packet for routing processing. The next arrived RREP packets are discarded simply. Consequently, a packet forwarding route is hijacked by a black hole route with high probability.

In order to solve this problem, SAODV uses only the second-arrived RREP packet for routing processing. Fig. 3 shows a mechanism of this countermeasure. (1) In this scheme, according to the original AODV procedure, a RREQ packet is first flooded. (2) Then, the fake RREP packet is first-arrived with high probability. (3) This RREP packet is simply discarded. (4) Next, the second-arrived RREP packet is hunted and used for routing. RREP packets arrived after the second one are simply discarded.

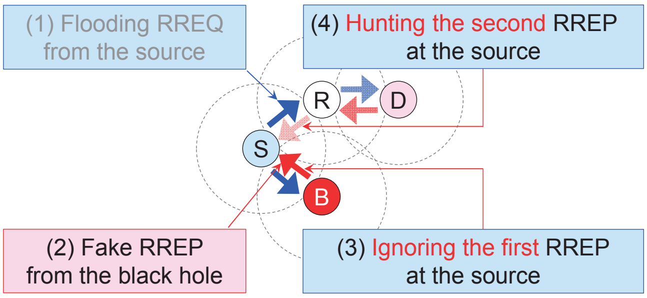
(1) Flooding RREQ from the source
(4) Hunting the second RREP at the source
R
D
S
B
(2) Fake RREP from the black hole
(3) Ignoring the first RREP at the source

Fig. 3 Overview of SAODV.

This simple modification may be effective countermeasure under the attacking conditions. However, under the normal conditions, its behavior seems a problem. Fig. 4 shows a mechanism of SAODV under this conditions. (1) A RREQ packet is first flooded. (2) Usually, only the single RREP may be returned from the destination host to the source host. (3) This only one RREP is simply discarded. Consequently, any route is not established. This behavior seems fatal. Thus, this problem should be solved.

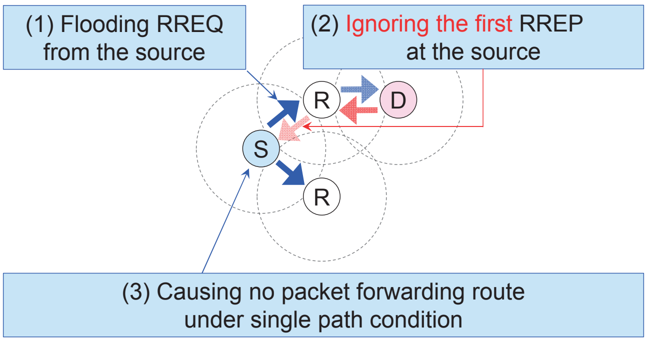
(1) Flooding RREQ from the source
(2) Ignoring the first RREP at the source
R
D
S
R
(3) Causing no packet forwarding route under single path condition

Fig. 4 Problem of SAODV.

4. Proposed Countermeasure

This section shows a novel countermeasure against black hole attacks as our proposal. First, the overview is shown. Then, a reachability checking scheme is proposed in order to solve misrouting problem. Finally, a reachability-information caching scheme is proposed for reducing control overhead of reachability check.

4.1 *Overview*

The problem of SAODV is that it does not use a first-arrived legitimate RREP packet. In order to solve this problem, RREP authentication seems attractive. However, it is difficult practically under the autonomous control environment. Thus, we deploy reachability check in place of direct RREP authentication.

The overview of this scheme is depicted in Fig. 5. This scheme is designed based on the original AODV. The difference is a reachability check procedure inserted after arrival of a RREP packet. (1) First, a RREP packet is returned to the source host. (2) Then, the source host checks reachability of the RREP-arrival direction to the destination. If reachability is assured, in succession, data packets are sent to this RREP-arrival direction. Else, the source host waits the next RREP packet. Then, it rechecks reachability of the next RREP-arrival direction.

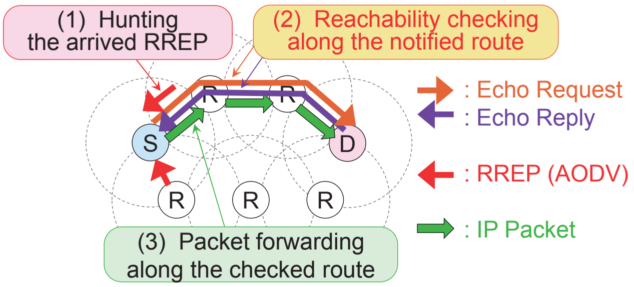
(1) Hunting the arrived RREP
(2) Reachability checking along the notified route
R
R
S
D
R
R
R
(3) Packet forwarding along the checked route
: Echo Request
: Echo Reply
: RREP (AODV)
: IP Packet

Fig. 5 Overview of the proposed scheme.

Due to those procedures, a black hole node can be bypassed surely from the packet-forwarding route. In addition, misrouting can be avoided in the normal conditions.

However, this control overhead may affect data forwarding performance. Thus, in order to mitigate this overhead, we further deploy reachability-information cache. In this scheme, multiple reachability check procedures toward the same direction are omitted. Here, the first result is shared between multiple check procedures for a while. If many packets are forwarded in a short period, this scheme behaves effectively. Consequently, data forwarding performance can be kept high.

4.2 *Reachability Check*

Reachability check is deployed in place of direct RREP authentication, as described above. Basically, this check is inserted after arrival of each RREP packet. Fig. 6 shows a procedure of reachability check under the normal conditions.

The first phase is the route-finding procedure based on the original AODV. (1-1) The source host floods RREQ packets to the destination host. (1-2) It receives the first-arrived RREP packet.

The second phase is the reachability check procedure inserted into AODV. This is the core part of the proposal. (2-1) The source host determines the packet forwarding direction temporarily using the arrived RREP packet. (2-2) It unicasts ICMP echo request to the destination host from the temporary direction. (2-3) It receives ICMP echo reply from the destination host. Thus, reachability check is succeeded.

The third phase is the packet forwarding procedure. (3-1) The source host sends data packets to the destination host from the checked direction.

Those processes effectively solve the problem of SAODV misrouting under the normal conditions.

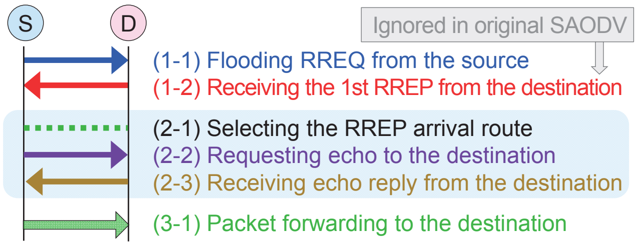
S
D
Ignored in original SAODV
(1-1) Flooding RREQ from the source
(1-2) Receiving the 1st RREP from the destination
(2-1) Selecting the RREP arrival route
(2-2) Requesting echo to the destination
(2-3) Receiving echo reply from the destination
(3-1) Packet forwarding to the destination

Fig. 6 Reachability checking under normal conditions.

On the other hand, Fig. 7 shows the procedure under the attacking conditions. The first phase is the same as that of the normal conditions. (1-1) The source host floods a RREQ packets to the destination host. (1-2) It receives the first-arrived RREP packet.

The second phase is little different from that of the normal conditions. (2-1) The source host determines a packet forwarding direction temporarily. (2-2) It unicasts ICMP echo request from this temporary direction to the destination host. (2-3) It does not receive ICMP echo reply from the destination host within a certain period. Thus, reachability check is failed.

In this case, a process goes back to the first phase for finding another route again. (1-3) The source host waits for another RREP packets and receives the second-arrived RREP packet. Here, note that the second packets may have been caching if it arrived immediately after the first packet arrival.

The third phase is the same as the second phase under the normal conditions. (3-1) The source host determines the packet forwarding direction temporarily. (3-2) It unicasts ICMP echo request to the destination host from the temporary direction. (3-3) It receives ICMP echo reply from the destination host.

If reachability check is failed in (3-3), a process goes back to the first phase again and processes are repeated. Else, a process goes to the fourth phase for data packet forwarding. (4-1) The source host sends data packets from the checked direction to the destination host.

Those processes solve effectively the problem of AODV misrouting under black hole attacking. As the result, the proposed countermeasure behaves appropriately under both normal and anomaly conditions. Here, the anomaly condition means that a black hole node is attacking.

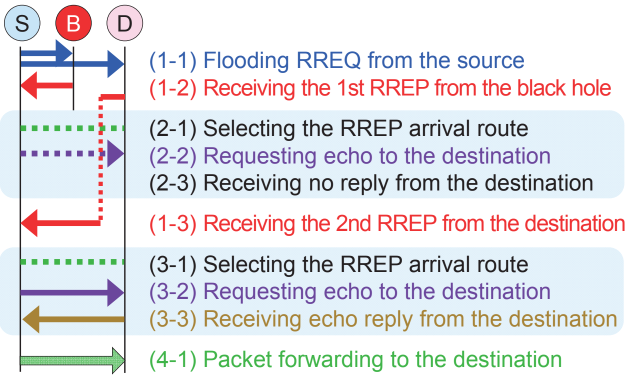
S
B
D
(1-1) Flooding RREQ from the source
(1-2) Receiving the 1st RREP from the black hole
(2-1) Selecting the RREP arrival route
(2-2) Requesting echo to the destination
(2-3) Receiving no reply from the destination
(1-3) Receiving the 2nd RREP from the destination
(3-1) Selecting the RREP arrival route
(3-2) Requesting echo to the destination
(3-3) Receiving echo reply from the destination
(4-1) Packet forwarding to the destination

Fig. 7 Reachability checking under anomaly conditions.

4.3 *Reachability-information Cache*

The proposed reachability check suppresses misrouting effectively. However, its overhead seems large in the normal conditions. In order to mitigate this overhead, we also deploy a reachability-information caching scheme.

Fig. 8 shows a procedure of our reachability check under the normal conditions. The overhead processes to be omitted are shown as the process (2-2) and (2-3).

In the initial stage, the whole processes should be performed. Then, the result of the check (the process (2-2) and (2-3)) is cached for a short time.

In the next stage, before the data packet transmission, the source host checks whether the corresponding cache is exist or not. When the cache exists, it is used for reachability checking. Consequently, the ICMP echo request/reply processes (the process (2-2) and (2-3)) are omitted. If the cache does not exit, the ICMP echo request/reply processes are fully executed and its result is cached.

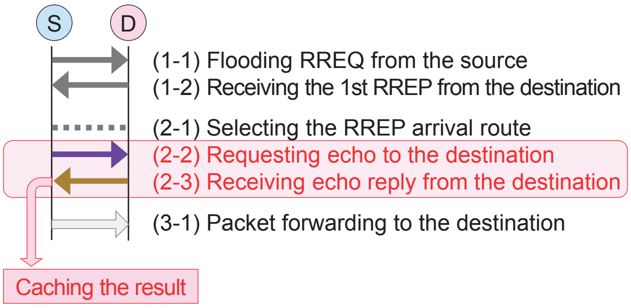
S
D
(1-1) Flooding RREQ from the source
(1-2) Receiving the 1st RREP from the destination
(2-1) Selecting the RREP arrival route
(2-2) Requesting echo to the destination
(2-3) Receiving echo reply from the destination
(3-1) Packet forwarding to the destination
Caching the result

Fig. 8 Processes to be omitted.

Fig. 9 shows how does cache work effectively. In this figure, the source host (S) and six destination hosts (D1-D4) are connected with each other using four relaying nodes (N1-N2, R, B). Here, the node (B) is a black hole.

The number of destinations (D1-D4) seems large. However, the number of the next-hop nodes (N1-N2) from the source (S) is small. This is because the packet forwarding route from the source (S) to the destinations (D1-D4) is tree-shaped logically.

From the viewpoint of the source (S), the destinations (D1-D2) are located behind the black hole (B). RREQ packets to those (D1-D2) are replied illegally by this black hole (B). Those faked RREP packets are reached via the next-hop (N1). Accordingly, received RREP packets via this node (N1) are faked with high probability.

On the other hand, the destinations (D3-D4) reply for RREQ packets directly. Those replied RREP packets are reached via the next-hop (N2). Consequently, received RREP packets via this node (N2) are legitimate with high probability.

According to those backgrounds, we can cache the result of ICMP echo request/reply as the reachability check result. In addition, we can use this result for the ensuing reachability checks directed to the same next-hop route.

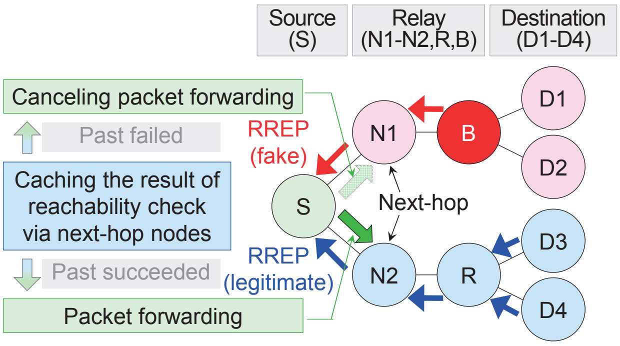

Fig. 9 Use of reachability-information cache.

5. Evaluation

This section shows evaluation using simulation. First, the overview is shown. Then, reachability, latency and throughput are compared between the conventional schemes and the proposed schemes. Finally, the results are summarized.

5.1 *Overview*

Our reachability checking scheme and reachability-information caching scheme were evaluated by way of simulation. Here, we call the former and the latter as AODV-RC and AODV-RC2, respectively. They are compared with AODV and SAODV from the viewpoint of reachability, latency and throughput. We used MATLAB as the simulation tool. In this simulation, our reachability checking function was implemented as shown in Table 1. The simulated network model is shown in Fig.10. A circle and the number in this figure show host location and host identification, respectively. Here, the black circle shows the black hole. Every hosts dynamically move around within 1 square kilometer area. The reachable range of radio wave is 250 meters. Other conditions are summarized in Table 2.

Table 1 Reachability checking algorithm.

```
1. Check D by flooding RREQ from S
2. Select receiving RREP arrival route
3. Check reply by sending request echo to D
   Then wait for replying from D
   (1) If received echo reply from D
         Then packet forwarding to D
   (2) If not received echo reply from
         Then (go to 2)
```

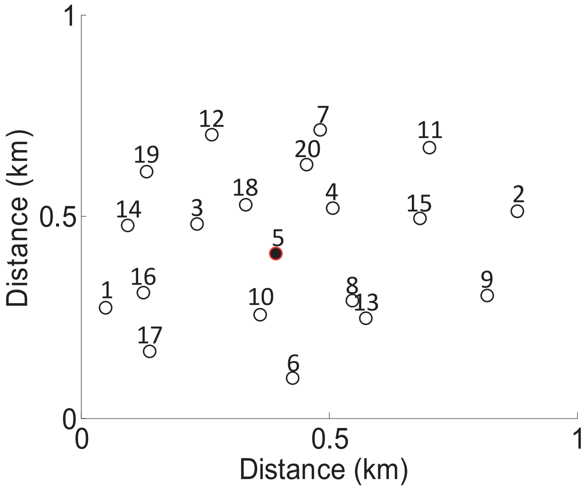

Fig. 10 Network model.

Table 2 Simulation parameters.

Parameter	Value
Number of nodes	20-50 nodes
Wireless protocol	IEEE 802.11
Packet length	512 bytes
Simulation period	1,000 seconds
Number of simulation trials	100 times

5.2 *Packet Delivery Ratio*

Packet delivery ratio was measured as the reachability evaluation. It is a ratio of the number of received packets at the destination to that of sent packets at the source in the whole network. Fig. 11 and Fig. 12 show the measured average ratio under the normal conditions and the anomaly conditions, respectively. In both figures, X-axis and Y-axis show the number of hosts in the network and average packet delivery ratio, respectively.

In Fig.11, under the normal conditions, SAODV shows the worst ratio. This is due to misrouting. Other schemes show almost the same ratio because of the same shortest routing.

On the other hand, in Fig.12, under the anomaly conditions, AODV shows the worst ratio. This is due to the black hole. SAODV shows better ratio than that of AODV. This is because the black hole is bypassed effectively. However, AODV-RC and AODV-RC2 show the best ratio because of the optimal routing achieved by means of reachability check.

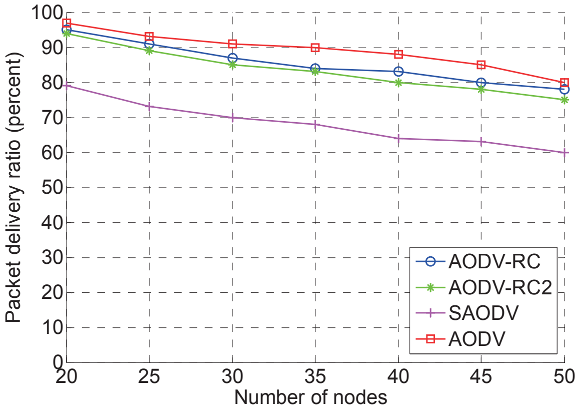

Fig. 11 Packet delivery ratio in normal conditions.

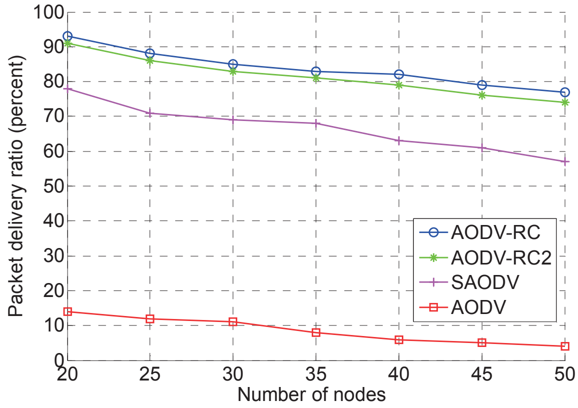

Fig. 12 Packet delivery ratio in anomaly conditions**.**

5.3 *Latency*

Latency here means the total delay of a routing procedure and a data forwarding procedure. Fig. 13 and Fig. 14 show the measured average latency under the normal conditions and the anomaly conditions, respectively. In both figures, X-axis and Y-axis show the number of hosts in the network and latency, respectively.

In Fig. 13, under the normal conditions, AODV shows the minimum latency, while SAODV shows the maximum latency. This is because AODV route is the shortest, while SAODV route is longer. The latency of AODV-RC is almost the same as that of SAODV. However, AODV-RC route is the shortest. This means that overhead of reachability check is large. The latency of AODV-RC2 is almost the same as that of AODV. This means that the reachability check overhead is mitigated effectively by means of reachability-information caching.

The features of Fig. 14 are almost the same as that of Fig. 13. This is because the latency can be measured only if data packets are forwarded successfully.

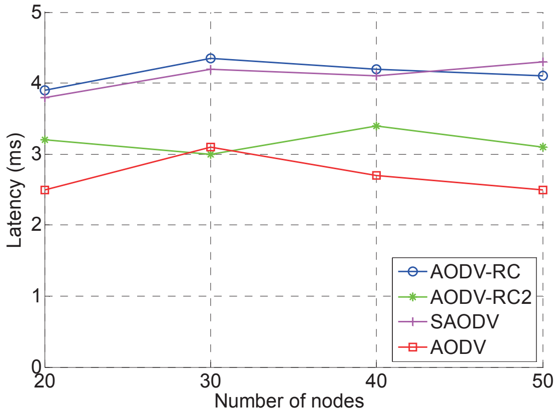

Fig. 13 Latency in normal conditions.

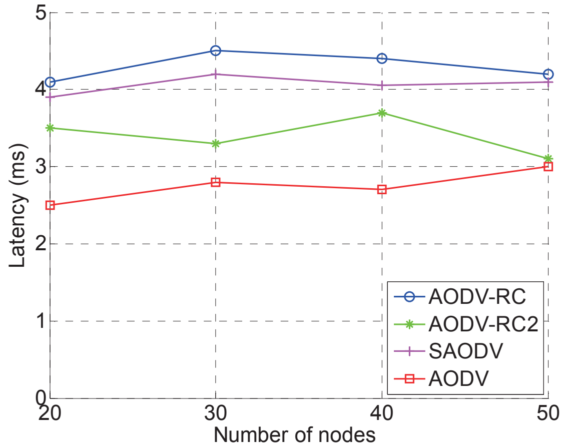

Fig. 14 Latency in anomaly conditions.

5.4 *Throughput*

Throughput here means the total amount of data that delivered successfully in the network during the simulation period. Fig. 15 and Fig. 16 show the measured average throughput under the normal conditions and the anomaly conditions, respectively. In both figures, X-axis and Y-axis show the number of hosts in the network and throughput, respectively.

In Fig. 15, under the normal conditions, AODV and SAODV show the best and worst throughput, respectively. This is because AODV achieves optimal routing, while SAODV causes misrouting. Although AODV-RC and AODV-RC2 also achieve optimal routing, their throughput is less than that of AODV. This is due to overhead of reachability checking. Since this overhead is mitigated in AODV-RC2, throughput of AODV-RC2 is better than that of AODV-RC.

On the other hand, in Fig.16, under the anomaly conditions, AODV shows the worst throughput due to the black hole. SAODV shows better throughput than that of AODV. This is the effect of bypassing the black hole. However, AODV-RC and AODV-RC2 show further better throughput because of their optimal routing achieved by means of reachability checking. In addition, AODV-RC2 shows the best throughput. This means that the reachability check overhead is mitigated effectively even under the anomaly conditions by means of reachability-information caching.

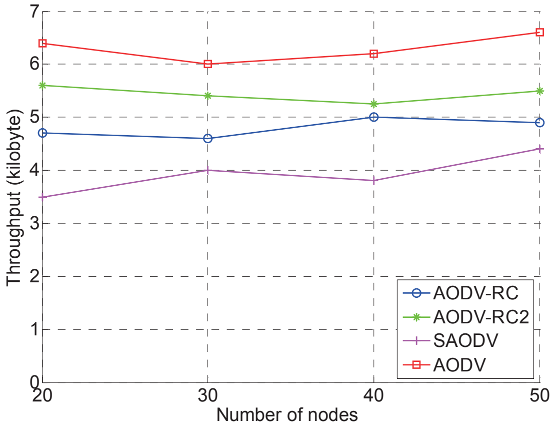

Fig. 15 Throughput in normal conditions.

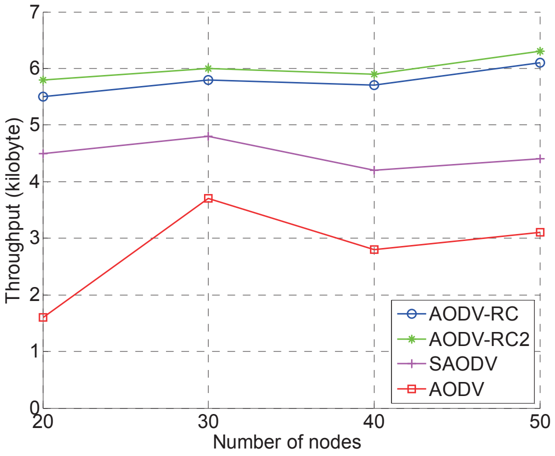

Fig. 16 Throughput in anomaly conditions.

5.5 *Summary*

The most important evaluation index is throughput because of the low-power and high throughput requirement for MANET. AODV is the best under the normal conditions, while AODV-RC2 is the best under the anomaly conditions. AODV-RC2 is also the second best under the normal conditions. In addition, the throughput difference is small. Consequently, we can say that AODV-RC2 is the current best countermeasure against black hole attacks on MANETs. This conclusion is also supported from the results of reachability evaluation and latency evaluation.

6. Discussions

In basic AODV routing, a RREP packet is unicasted from the destination host to the source host. Consequently, a packet forwarding route is determined uniquely. However, this feature is fatal against black hole attacks. This is because multipath routes are indispensable for bypassing a black hole node. In this section, we discusses about multipath routing.

6.1 *Multipath routing in original AODV*

Relay hosts may know the route to the final destination. In AODV routing, such hosts can independently send a RREP packet in place of the destination. Consequently, multiple RREP packets may be returned to the source host from the different directions. Those RREP packets are useful to achieve multipath routing.

The mechanism of AODV multipath routing is schematically shown in Fig. 17. In this mechanism, first, the source host (S) floods a RREQ packet toward the destination host (D) via relay hosts (R1-R5). The flooded RREQ packets are reached to relay hosts (R2, R5). Those hosts are located near the destination (D) and thus they (R2, R5) know the route to the destination (D) with high probability. (1) Then, they (R2, R5) respond to this RREQ packet using a RREP packet independently. (2) Accordingly, multiple RREP packets are returned to the source (S) via the different routes.

The source (S) that receives multiple RREP packets selects an appropriate RREP packet for data packet forwarding. Typically, a RREP packet corresponding to the shortest route is selected. In addition, another RREP packets can be also selected to use the alternative routes.

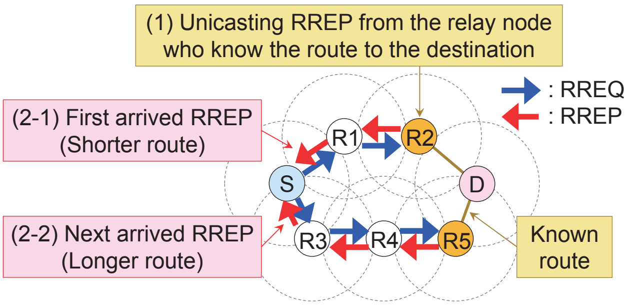
(1) Unicasting RREP from the relay node who know the route to the destination
(2-1) First arrived RREP (Shorter route)
(2-2) Next arrived RREP (Longer route)
: RREQ
: RREP
S
R1
R2
D
R3
R4
R5
Known route

Fig. 17 AODV multipath routing.

6.2 *Multipath routing in conventional countermeasure*

The RREP packet corresponding to the shortest route is arrived first with high probability as shown in Fig. 18. (1) This RREP packet is simply discarded at the source (S) in SAODV routing. (2) Next, the second-arrived RREP packet is hunted and used for data packet forwarding. Then, data packet can be forwarded to the destination even in the normal conditions.

However, the route determined by the second-arrived RREP packet is not the shortest but the second shortest. Consequently, data forwarding latency increases and the whole network throughput decreases.

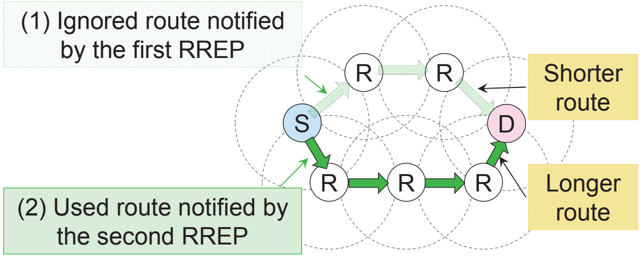
(1) Ignored route notified by the first RREP
(2) Used route notified by the second RREP
Shorter route
Longer route
S
R
R
D
R
R
R

Fig. 18 SAODV multipath routing.

6.3 *Multipath routing in proposed countermeasure*

The proposed countermeasure under multipath shown in Fig. 19. (1) In our scheme, at the source (S), the first-arrived RREP packet can be used even in the normal conditions. (2) This is enabled by way of reachability checking. (3) Thus, data packets can be forwarded along the shortest route. However, this RREP packet is discarded when reachability check is fail. In this case, the second-arrived RREP packet is hunt to use the alternative route. This means that a black hole node can be bypassed effectively. Accordingly, data forwarding latency is maintained low and the whole network throughput is kept high.

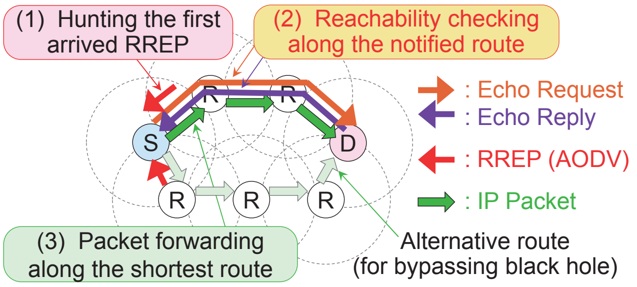
(1) Hunting the first arrived RREP
(2) Reachability checking along the notified route
: Echo Request
: Echo Reply
: RREP (AODV)
: IP Packet
(3) Packet forwarding along the shortest route
Alternative route (for bypassing black hole)
S
R
R
D
R
R
R

Fig. 19 Proposed multipath routing.

6.4 Countermeasure against advanced attacks

Once our proposal has been applied, black hole nodes may evolve so as to return fake ICMP echo replies. To solve this problem, host applications also need to check reachability. Accordingly, every arrived RREP packet is checked their reachability by the received host regardless of the check results. Then, a host will replace the failure communication route to the available one if the host application detects an initial-communication failure. In order to achieve this solution, the socket interface between the network function and application functions needs to be extended so as to support failure notifications.

Some black hole nodes may further evolve to act as phishing servers. To solve this problem, certification of the destination host is necessary. A public and private key pair seems attractive for achieving this solution. However, in this paper, balancing both good convenience and strong security optimally in MANETs is out of scope. It is an important future issue.

7. Conclusion

An AODV-based MANET is attractive as a future device network because of its high mobility feature. The essence of MANET is economical routing in order to achieve low-power and high-throughput features. The biggest threat for such features is a black hole attack that interferes optimal routing. The conventional countermeasure is effective against such an attack, while it does not work well under the normal conditions.

The proposed countermeasure solves this problem by means of a reachability checking scheme. This scheme is based on ICMP echo request/reply and supports optimal AODV routing. However, this simple solution may loose low-power feature due to its large control overhead. Then our countermeasure also deploys a reachability-information caching scheme. In our scheme, reachability check using ICMP is executed once and the result is cached. This cache is used to check reachability for the ensuing packet routing. Consequently, the cache effectively mitigates overhead of ICMP-based reachability checking.

As the result, our countermeasure maintains low-power and high-throughput features against black hole attacks.

References

[1] S. Misra, I. Woungang and S. C. Misra, "Guide to Wireless Ad Hoc Networks" ISBN-13: 978-1848003279, Springer, 2009.

[2] Y. Kawamoto, H. Nishiyama, N. Kato, N. Yoshimura and S. Yamamoto, "Internet of Things (IoT): Present State and Future Prospects" IEICE Trans. Info. & Syst., Vol.E97-D, No.10, pp.2568-2575, Dec. 2014.

[3] S. Yousefi, M. S. Mousavi and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives" Proc. 6th Int. Conf. ITS Telecommun., pp761-766, Jun. 2006.

[4] X. Wu, M. Mazurowski and Z. Chen, "Emergency message dissemination system for smartphones during natural disasters", ITST, 2011.

[5] R. Misra and C. R. Mandal, "Performance comparison of AODV/DSR on-demand routing protocols for ad hoc networks in constrained situation" Proc. ICPWC 2005, pp.86-89, 2005.

[6] M. Puray and P. Palod, "Black-Hole Attack in MANET: A Study" IJARCET, Vol.5, No.3, pp.597-601, Mar. 2016.

[7] A. A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks" Proc. ICPC2015, 2015.