1-1-2018

An Enhanced AODV Protocol for Avoiding Black Holes in MANET

Qussai M. Yaseen
Jordan University of Science and Technology

Monther Aldwairi
Jordan University of Science and Technology

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 134 (2018) 371–376

Procedia Computer Science

www.elsevier.com/locate/procedia

The 5th International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2018)

An Enhanced AODV Protocol for Avoiding Black Holes in MANET

Qussai M. Yaseen[a*], Monther Aldwairi[a,b]

[a]Computer and Information Technology College, Jordan University of Science and Technology, Irbid, Jordan 22110
[b]College of Technological Innovation, Zayed University, Abu Dhabi, UAE

Abstract

Black hole attack is one of the well-known attacks on Mobile Ad hoc Networks, MANET. This paper discusses this problem and proposes a new approach based on building a global reputation system that helps AODV protocol in selecting the best path to destination, when there is more than one possible route. The proposed protocol enhances the using of watchdogs in AODV by collecting the observations and broadcasting them to all nodes in the network using a low overhead approach. Moreover, the proposed protocol takes into account the detection challenge when a black hole continuously moves.

Keywords: Black hole; MANET; AODV; Information Security.

1. Introduction

Wireless sensor networks (WSNs) consist of cheap, battery-powered and simple processing devices that are called sensor nodes. Sensor nodes are equipped with wireless radio devices that are used to form highly distributed ad hoc networks. Typically, sensor nodes are used for monitoring weather conditions such as temperature, humidity, etc. or monitoring a physical phenomenon. For example, WSNs are used in military, building and industrial

[*] Corresponding author. Tel.: + 962 (0) 2 7201000; fax: + 962 (0) 2 7095123.
E-mail address: qmyaseen@just.edu.jo

10.1016/j.procs.2018.07.196

monitoring and automation1. Ad hoc networks are nodes communicating and storing data wirelessly without requiring physical infrastructure. They reduce time and money requirements, and therefore the network can be up and running quickly. Ad hoc network is based on multi-hop communication, where nodes collaborate to deliver the sent packet to the destination.

Mobile ad hoc network (MANET) consists of a number of mobile nodes that do not need any infrastructure to maintain the network connection. All nodes in MANET may work as a sender or receiver of a packet, or as a router. MANET is used in many areas, such as disaster areas, military fields, personal area networks, etc. The mobile or dynamic nature of MANET offers some advantages over non-mobile ad hoc network, such as there is no single point of failure in this type. However, special protocols should be used to deliver packets to destination since known paths from source to destinations change overtime in dynamic topologies. Three categories of protocols are used in MANETs, which are proactive (table-driven), reactive (on-demand) and hybrid protocols.

Proactive or table-driven protocols maintain an up-to-date topology (map) for the entire network. Therefore, when a node wants to send a packet to a destination, the route is known and already exists in the source node's packet table. Proactive protocols are classified into link-state or distance vector protocols. The advantage of link-state protocols over distance vector protocols is the fast convergence. However, it needs more control traffic. OLSR2 is an example of proactive protocols.

Reactive routing protocols do not maintain a topology of the network; a route to a destination is built on demand. For this purpose, a source node needs to broadcast request searching for a route to a destination. Intermediate nodes in the MANET forward the request and help in building a route to the destination. AODV and DSR3 are examples of reactive protocols.

Hybrid (reactive/proactive) protocols, such as ZRP4 and WRP5, combine both proactive and reactive approaches; they use proactive approach for finding zone neighbors and reactive approach to discover routes between zones. A neighboring zone is maintained by regularly sending a hello message to neighbors to check whether they are alive. In this type of protocols, routes to neighbors are immediately available when needed. Based on the assumption that the largest part of the traffic is directed to nearby nodes in ad hoc networks, hybrid protocols reduce the delay and traffic needed to build a route when sending a packet to neighboring nodes, while they build a route to far nodes on demand only.

MANET, as in wired and wireless networks, face many security issues such as routing table overflow, poisoning, wormhole, snooping, packet replication and denial of service (DoS) attacks. A popular security issue in MANET is the black hole problem. A black hole node is a node that claims itself as the shortest path to the destination, however, when it gets a packet to forward it to the destination, it drops it. Black hole attacks could be single or collaborative. In single black hole attacks, one node behaves independently and drops packets that should be forwarded to neighbors. In collaborative black hole attacks, some malicious nodes cooperate together to drop packets to avoid the detection systems. Many detection schemes have been proposed to detect black hole attacks for various protocols in MANETs.

This paper discusses the problem of black hole detection in MANET using an enhanced version of AODV protocol. The contribution of the paper is summarized as follows.

- The paper introduces an enhanced version of the AODV for routing packets in MANET.
- The new protocol prevents black hole node or misbehaving nodes from dropping packets by using an up-to-date reputation table for all nodes in MANET.
- The new protocol prevents black hole problem with a reasonable traffic overhead by using reputation aggregators.
- A detailed algorithm of the new protocol has been added and well-discussed.

The rest of the paper is organized as follows. The following section discusses some of the related work. Section 3 introduces the proposed protocol. Finally, section 6 concludes the work.

2. Related Work

Different prevention and detection approaches have been proposed for single and collaborative black hole attacks. Sun et al. [1] proposed a neighborhood-based approach to detect black holes, and routing recovery approach to build a good path to the destination. Their approaches are used for detecting single black holes in AODV protocol, therefore, it is not suitable for collaborative black hole attacks. Al-Shurman et al.[2] proposed two solutions for detecting single black holes in AODV protocol. The first solution considers redundant paths to a destination. The work combines the use of possible redundant paths with building a reputation system that can be used to choose the best path among redundant paths. We should mention here that this approach does not aim to avoid black holes only when sending packets, but aims at avoiding devices that cannot forward packets in a good manner too due to many reasons such as noise and environment conditions. The second solution uses a unique sequence number in packets. This number is accumulated and used by sender nodes to check whether there is a malicious node or not.

Tamilselvan et al.[3] proposed a time-based threshold detection scheme to detect single black holes in AODV protocol. The proposed approach stores a packet's sequence number and the received time to count the timeout value of the first route request. Using this information and a threshold value, the approach can check whether a route is valid or not. Djenouri and Badache [4] proposed an approach of two phases, which are the monitoring and detection phases for detecting single black hole in AODV. In the monitoring phase, they used a random two-hop ACK for monitoring the communication among nodes in MANET. The authors used a Bayesian approach for detecting misbehaving nodes in the detection phase. The authors claimed that the approach achieves a high true detection rate of about 100%.

Kozma et al.[5] used an approach that uses audit nodes and bloom filters to detect single black hole attacks in DSR protocol, while Raj and Swadas [6] used a new control packet called ALARM to detect the problem for AODV protocol. Jaisankar et al.[7] added a new field, called field_next_hop, to the RREP packet and used a black identification table to detect misbehaving nodes for AODV protocol. Mistry et al. [8] added a new table, a new timer and a new variable to the AODV protocol, and modified functions to detect black holes. Su [9] used an intrusion detection system by injecting an anti-black countermeasure in selected IDS nodes since there is no centralized infrastructure device in MANET.

3. The Proposed Protocol

This paper proposes a protocol that leverages the advantages of both protocols, AODV and OLSR, and overcomes their disadvantages when using the Watchdogs and Pathrater approach. The proposed model consists of three major parts, which are Gathering Reputation Values, Computing Reputation Values, and Selecting Best Route.

3.1 Gathering Reputation Values

The reputation values that are collected about a node using Watchdogs and Pathrater approaches depend on individual monitoring by the node's neighbours. As discussed previously, these values form a partial knowledge about whether a node is malicious or not. However, sharing this information among nodes in the network to build a global reputation system can help in more precise decisions about whether a node is malicious or not. Exchanging the observations about nodes should be performed in a manner that has the least effect on the network traffic and performance. Figure 1 shows the proposed approach for sharing reputation values. The steps of gathering reputation values are summarized as follows.

A. Each node monitors the traffic it sends to its neighbors as well as the traffic out of its neighbors, and keeps the reputation value of each node it monitors. The reputation value of a neighbor X that is monitored by a node Y is calculated as follows[15].

$$R(X) = SP(X)/FP(X) \tag{1}$$

Where R(X) denotes the reputation of X, SP(X) denotes the number of sent packets to X by Y, and FP(X) denotes the number of forwarded packets by X.

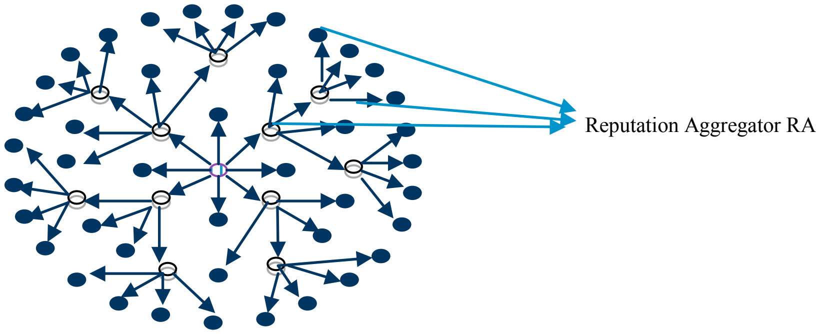

Fig. 1. Exchanging reputation information among nodes in the proposed protocol.

B. Each node selects a set of Reputation Aggregators (RAs) from its 1-hop neighbors. The RA set of a node, say X, should cover all 2-hop neighbors of X. Without loss of generality, only the RA set of X is allowed to forward the X's table of reputation values to other nodes. This process eliminates the redundant traffic that may be posed when all neighbors of X, not only RAs, are allowed to forward X's reputation table. Hence, since X's RA set covers all 2-hop neighbors of X, they should get a copy of X's reputation table. The same process is repeated by all nodes until each node in the MANET gets a copy of the reputation nodes of all other nodes.

C. Each node updates its table of reputation values according to the new reputation tables it receives from RAs. After convergence, each node should have a complete view of the reputation values of all nodes in the network.

D. The updates on reputation values of nodes should be sent once exist. The updates may be broadcasted using three approaches, which are as follows.
   - The *Immediate Broadcasting Approach*: In this approach, a watchdog sends the updates once a change in the reputation value of a monitored node exists. This approach offers a high precision in black hole detection since the tables of reputation values in nodes are updated immediately. However, the high rate of broadcasting updates increases the network traffic.
   - The *Time Window Broadcasting Approach*: In this approach, the updates are collected and broadcasted every preset time interval, i.e. every 4 minutes. This approach reduces traffic overhead, but some black hole may arise and drop packets before they are detected. However, the severity of the aforementioned drawback depends on the length of the time window. Therefore, the tradeoff between traffic reduction and the black hole detection should be considered.
   - The *Light Broadcasting Approach:* This approach collects updates and broadcasts them when the network has low traffic. Since the broadcasting rate depends on the network traffic, the performance of the network should not be degraded. However, the detection precision of black hole nodes is high when network traffic is low, meanwhile, it is low when the network traffic is high.

Choosing the appropriate broadcasting approach may depend on the network environment. For example, when the transmission rate of nodes is low, the immediate broadcasting approach may be used since the updating rate in reputation values is low.

3.2 Updating Reputation Values

Two issues should be handled when dealing with reputation values updates. First, how to compute the updated reputation value of a node? Second, when more than one watchdog sends the updates of a node's reputation, what values should be considered?

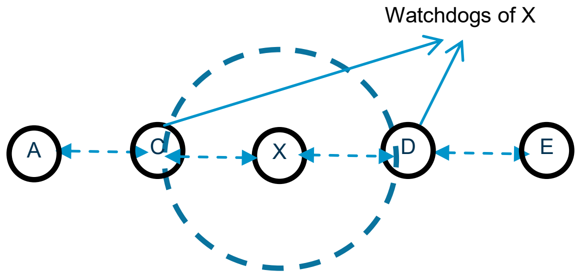

Fig. 2. Computing Updated Reputation Values.

To discuss the first issue, consider Figure 2, where the monitored node is X, and the watchdogs of X are C and D. The watchdogs of X are responsible for computing the updated reputation value of X. Two values should be considered, which are the stored (old) reputation value of X in the watchdog nodes (C and D), and the current computed reputation value that is based on the current forwarding and receiving of packets by X. C and D compute the current reputation value of X based on Formula 1. Next, they use this value and the old reputation value stored in their reputation tables to compute the updated version of the value. Formula 2 shows how to compute the updated value.

$$UR(X) = W_c * R(X) + W_o * OR(X) \qquad (2)$$

Where UR(X) denotes the updated reputation value of X, W_c denotes the weight of the current computed reputation value of X, R(X) the current computed reputation value of X, W_o the weight of the old reputation value of X, OR(X) is the old reputation value of X. Hence, $W_c + W_o = 1$.

Selecting the appropriate weight values, W_c and W_o, is very important in detecting black hole nodes. Assigning a very high value to W_c (very low value to W_o) may enable some nodes, that were considered as black hole nodes in the past in other locations, to get a high reputation quickly in new locations when moving and get a fast chance to drop packets. Meanwhile, assigning a very high value to W_o (very low value to W_c) may prohibit some benign nodes, that suffered malfunctions in the past and dropped packets due to environment conditions, from getting back quickly and participate in sending readings. Therefore, these values should be assigned such that the approach can detect and prevent black hole nodes when moving to new locations, and give the benign nodes a new chance to participate in sending values when the environment conditions resolved.

When the watchdogs update the reputation values of the monitored node(s), they broadcast these updated values to other nodes in the network. A node, say X, may receive multiple updated values for the same monitored node, say Y. In this case, X should select the most recent value. To do this, the broadcasted updated values by watchdogs should have a time stamp that enable X from selecting the most recent value.

3.3 Selecting the Best Route

Selecting the best path for sending or forwarding a packet is the ultimate goal of routing protocols in MANET. When a node, say X, needs to send a packet to a destination, say Y, X may get multiple paths to Y. In this case, X should choose that most reliable path based on the reputation values of nodes in the paths. This process does not avoid black hole nodes only; it avoids benign nodes that face some environment conditions that prevent them from forwarding packets properly.

Using the reputation table, each node should have knowledge about every node in the network. This offers a great advantage in avoiding black holes. Moreover, the reputation tables are updated regularly which offers nodes the most updated reputation values of moving nodes. This reduces the risk that comes from black holes that move among different areas to avoid detection.

The proposed approach aims at providing the required knowledge for each node in MANETs to avoid black holes in dynamic environments, where nodes are moving continuously. It provides a light approach to broadcast reputation values among nodes to reduce the network overhead.

Conclusions and Future Work

The paper has presented a new enhanced protocol of AODV that can detect and avoid black holes in MANETs. The proposed protocol uses a global reputation table in each node. A reputation table is built using watchdogs' observations, which are distributed to all nodes using a low overhead approach. The reputation tables enable nodes to choose the best path with the best reputable nodes when there is more than one route to a destination. This advantage may be leveraged by nodes in MANETs not only to detect and avoid black holes, it enables them to detect and avoid benign nodes that may face fatal environment conditions that prevent them from working correctly. As future work, we aim at conducting experiments that test the performance and the scalability of the proposed protocol.

Acknowledgements

This work was supported by Zayed University Research Office, Research Cluster Award #R17079.

References

[1] Sun B, Guan Y, Chen J, Pooch UW. (2003). "Detecting Black-hole Attack in Mobile Ad Hoc Networks." *In Proceedings of the 5th European Personal Mobile Communications Conference*, Glasgow, United Kingdom.

[2] Al-Shurman M, Yoo S-M, Park S. (2004). "Black Hole Attack in Mobile Ad Hoc Networks." *In Proceedings of the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42)*, Huntsville, Alabama.

[3] Tamilselvan L, Sankaranarayanan V. (2007). "Prevention of Blackhole Attack in MANET." *In Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, Sydney, Australia.

[4] Djenouri D, Badache N. (2008). "Struggling Against Selfishness and Black Hole Attacks in MANETs." *Wireless Communications & Mobile Computing. Vol* 8, NO 6, pp 689–704.

[5] Kozma W, Lazos L. (2009). "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits." *In Proceedings of the 2nd ACM Conference on Wireless Network Security*, Zurich, Switzerland.

[6] Raj PN, Swadas B. (2009). "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET." *International Journal of Computer Science*, Vol 2, PP 54–59.

[7] Jaisankar N, Saravanan R, Swamy KD. (2010).A Novel Security Approach for Detecting Black Hole Attack in MANET. *In Proceedings of the_International Conference on Recent Trends in Business Administration and Information*, Thiruvananthapuram, India.

[8] Mistry N, Jinwala DC, IAENG, Zaveri M. (2010). "Improving AODV Protocol Against Blackhole Attacks." *In Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong.

[9] Su M-Y. (2010). "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems." *IEEE Computer Communications,* Vol 34, No 1. PP 107–117.

[10] Varshney T., Sharmaa T., Sharma P. (2014). "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network." *In Proceedings of* 4th *International Conference on Communication Systems and Network Technologie*.