

# Performance Evaluation of Black Hole Attack Under AODV in Smart Metering Network

Yanxiao Zhao<sup>(✉)</sup>, Suraj Singh, Guodong Wang<sup>(✉)</sup>, and Yu Luo

Department of Electrical and Computer Engineering, South Dakota School of Mines  
and Technology, Rapid City 57701, USA  
{yanxiao.zhao, guodong.wang}@sdsmt.edu

**Abstract.** In this paper, we thoroughly investigate the impact of black hole attacks under Ad hoc On-Demand Distance Vector (AODV) routing in smart metering network. Specifically, the impact of black hole attack is fully examined by adjusting AODV parameters such as Hello message interval, route lifetime and positions of malicious meters, which have been under explored so far. Two critical performance metrics including packet delivery ratio and end-to-end delay are used to measure the impact. Extensive simulations are conducted in a topology based on an actual suburban neighborhood. Simulation results demonstrate that by carefully adjusting AODV parameters, it increases resistance against black hole attack. The position of malicious meters also plays a critical role to prevent black hole attack and is studied as well.

**Keywords:** Smart metering network · Black hole attack · AODV · Throughput · End-to-end delay

## 1 Introduction

Smart grid is generally referred to the next-generation power system that fully integrates high-speed and two-way communications. To evolve from a legacy power system to smart grid successfully, smart meters play a critical role because they are capable of recording consumption of electricity, gas and water for monitoring and billing. It is reported that nearly 50 million networked smart meters, about 43% of the county, have been installed and are running across USA as of July 2014 [1]. This number is expected to continually rise in the near future.

The security issue of smart grid heavily impacts its performance and has drawn considerable attention from academia, industry and government. Specifically, a variety of security attacks including denial of service, spoofing, and eavesdrop deserve an in-depth investigation in the context of smart grids. In this paper, we focus on black hole attack, which is one kind of denial of service and severely impairs the performance of a smart metering network.

A smart metering network is typically a wireless mesh network that consists of a data aggregation point (DAP) and a large number of smart meters [2–4]. The DAP is responsible for collecting information from smart meters. Some

smart meters have to serve as relay nodes to help deliver information to the DAP through multiple hops. During a black hole attack, a malicious meter discards packets from other meters instead of relaying packets as expected. This could occur due to a compromised meter from various causes.

Since a smart metering network is essentially a multi-hop network, a routing protocol is required to find the best route to the DAP for each smart meter. Ad hoc On-Demand Distance Vector (AODV) Routing is a widely-used protocol for mobile and wireless ad hoc networks, which is also recommended in the smart metering network [5]. Therefore, we adopt AODV as the routing protocol and evaluate black hole attacks under AODV in smart metering network.

In the literature, the impact of malicious meters has been studied for black hole attack under AODV including the impact of the number of malicious meters [6, 9]. Distinct from the existing work, our paper aims at carrying out a comprehensive investigation for the effect of malicious meters on network performance including Hello packet interval, route lifetime and positions of malicious meters, which have received limited attention. The performance metrics including packet delivery ratio (PDR) and end-to-end delay will be calculated to measure the impact on system performance.

In brief, the main contributions of this paper are summarized as below.

- Black hole attacks are simulated by modifying AODV functions to generate a fake route reply with a high sequence number and a low hop count. Data packets sent by source meters will be simply discarded by the malicious meters.
- The performance under black hole attacks is thoroughly evaluated by adjusting several factors. Specifically, the impact of AODV parameters including Hello message interval and route lifetime as well as positions of malicious meters are fully examined. To the best of our knowledge, it is the first time to conduct such a comprehensive investigation of black hole attacks under AODV in the context of smart metering network.
- Extensive simulations are conducted in a topology based on an actual suburban neighborhood in Rapid City, SD, USA. Simulation results show that performance varies when changing AODV parameters. By carefully adjusting AODV parameters, it increases resistance against black hole attack. In addition, the position of malicious meters affects networking performance and is examined as well. Findings from simulation will shed light on improving security in smart metering networks including malicious meters detection and robust routing protocol design.

The rest of the paper is organized as follows. Section 2 presents how to simulate the black hole attacks under AODV. The simulation setup and results are presented in Sects. 3 and 4, respectively. Concluding remarks are made in Sect. 5.

## 2 Black Hole Attack in Smart Metering Network

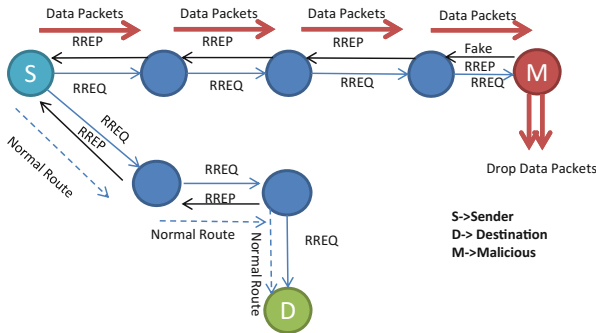
In this section, we will present how to trigger the black hole attacks under AODV in smart metering network. The AODV routing protocol will be briefly introduced followed by how to simulate black hole attacks under AODV.

### 2.1 AODV Routing Protocol

AODV is a reactive routing protocol designed to find a route between a source and a destination. In AODV, multiple types of messages are used, e.g., Route Request (RREQ), Route Reply (RREP), Route Error (RERR) and Hello message [7]. The source node initiates a route request RREQ and intermediate nodes are responsible for forwarding the RREQ message until the message is delivered to the destination node or an intermediate node that has a fresh route to the destination. In the latter case, the intermediate node sends a reply, i.e., RREP message back to the source node. After a route is established, the source and destination establish a communication and start transmitting data packets. When a link is broken, RERR message is sent to all nodes to notify a lost of link. Hello messages are used by nodes to monitor and detect links to neighbors. Once a node fails to receive Hello messages from its neighbor, a down link is detected.

### 2.2 Black Hole Attack Under AODV

Black hole attack falls into the category of Denial of Service (DoS) in which a malicious node exploits the route discovery process of AODV and advertises itself the shortest path to the destination. Malicious nodes on receiving route request initiated by a source node, replies with a fake RREP. The source node then forwards data packets to the malicious node which drops all the packets instead of forwarding. In our paper, malicious meters will send a tampered RREP that has 1 as the value of hop count and an extremely high value of destination sequence

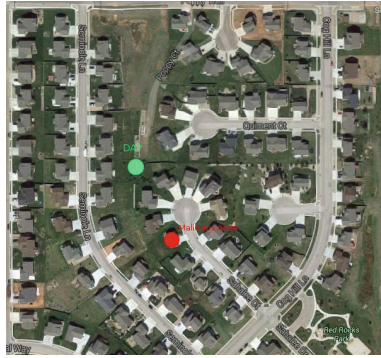


**Fig. 1.** Black hole attack under AODV: the malicious meter tricks the sender to send data packet towards itself and then drop the packets

number because a RREP message with a higher destination sequence number is always considered as a fresh route. Figure 1 illustrates the effect of black hole attack under AODV. It can be seen that with a malicious meter, the normal route is not adopted. Instead, the malicious meter misleads the source/sender to send data towards itself by relying with a higher destination sequence number and then drops the sender's packets. As a result, the performance of sender's PDR is severely degraded.

### 3 Simulation Setup and Performance Metrics

In this section, a simulation platform is set up using a popular Network Simulator 3 (NS3). To imitate a real smart metering network, a suburban neighborhood with 100 houses is selected from Rapid City, South Dakota, USA, as shown in Fig. 2.



**Fig. 2.** An actual suburban neighborhood selected from Rapid City, SD (color figure online)

It is assumed that each house installs a smart meter and a DAP is placed at the center of this neighborhood, which is marked as a green dot. In our simulations, the geographical information of this real neighborhood is imported to NS3 and the resulting smart metering network is created accordingly. The longitudes and latitudes of houses are obtained from Google map and the distance between any two smart meters is calculated by Haversine formula [8], presented by Eq. (1).

$$\begin{aligned}
 \Delta lat &= |lat2 - lat1| \\
 \Delta lon &= |lon2 - lon1| \\
 a &= \left(\sin\left(\frac{\Delta lat}{2}\right)\right)^2 + \cos(lat1) \times \cos(lat2) \times \left(\sin\left(\frac{\Delta lon}{2}\right)\right)^2 \\
 c &= 2 * \arctan 2(\sqrt{a}, \sqrt{1-a}) \\
 d &= R \times c
 \end{aligned} \tag{1}$$

where  $R$  is 6373 km, the radius of the earth.

IEEE 802.11 is recommended as a promising option for smart metering neighborhood network and we adopt IEEE 802.11 for smart meters as well [3]. The transmission range of the smart meters is set to 50 m. To achieve the coverage distance of 50 m for each station, Eq. (2) is utilized [12] as follows.

$$P = \left( \frac{4\pi D}{0.12476} \right)^2 X 10^{-12.5}, \quad (2)$$

where  $P$  is the transmission power and  $D$  is the coverage distance, which is 50 m in our paper.

The transmission pattern is carefully scheduled so that every smart meter periodically sends data to the DAP with 10 s interval between consecutive smart meters. AODV is chosen as the routing protocol for this scenario. The major parameters for the simulation setup are listed in Table 1.

**Table 1.** Specific parameters for simulations

Parameter	Attributes
Number of DAP	1
Number of smart meters	100
Packet size	1024
Transmission range	50 m
Routing protocol	AODV
Mobility model	Static
Traffic	Constant bit rate
MAC/PHY	IEEE 802.11b

To evaluate the black hole attacks under AODV, two widely used performance metrics [10, 11] will be examined and they are presented in the following.

- Packet Delivery Ratio (PDR): the ratio of the successfully delivered packets compared with the total packets that have been sent. It is formulated as:

$$PDR = \frac{\sum \text{number of packet received}}{\sum \text{number of packet sent}}$$

- End-to-end Delay: the average time taken by a data packet transmitted from a source to the destination. It is comprised of the delay caused by route discovery process and the queue in data packet transmission.

$$Delay = \frac{\sum (\text{arrival time} - \text{sent time})}{\sum \text{number of successful transmission}}$$

Note that the end-to-end delay is counted only for the successfully delivered data packets.

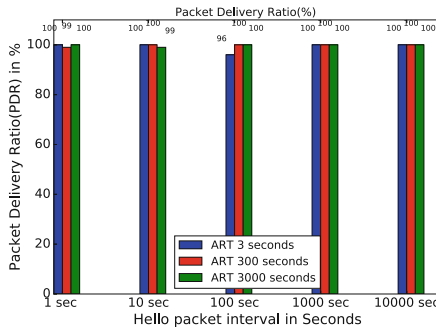
## 4 Simulation Results

In this section, extensive simulations are carried out to evaluate the impact of black hole attack under AODV protocol based on the topology shown in Fig. 2. The objective of the simulation is to evaluate how different parameters, such as Hello packet interval and Active Route Timeout (ART), affect the PDR and end-to-end delay of smart metering network in presence and absence of a black hole attack. In AODV, ART refers to as the rout state hold time, which means after such a time period nodes will remove the route states [12]. From simulation results, we attempt to draw general conclusions and provide insights how to choose an appropriate parameter to achieve a desirable performance.

In the simulation, we set three different values for ART, which are 3 s (i.e., the default value in AODV), 300 s and 3000 s. Note that when ART = 3000 s, all of the smart meters will not change route states for the entire simulation duration.

### 4.1 Effect of Variation of ART and Hello Packet Interval on PDR

First, the impact of ART and Hello packet interval on PDR is evaluated with and without malicious meters. Without malicious behaviors, all meters behave normally and send data successively to the DAP. Figure 3 demonstrates the average PDR of all senders with varied ART and Hello packet interval without malicious meters. It can be observed that the PDR is about 100% for all settings and no significant difference is observed when ART and Hello packet interval are changed. This result is expected since the meters are stationary and changing ART value and Hello interval will not significantly affect the PDR.



**Fig. 3.** Average packet delivery ratio without malicious activities

Figure 4 shows the PDR of the same topology under a single malicious meter, whose position is marked in Fig. 2. The PDR falls down to 57% for the default AODV setting (i.e., Hello packet interval = 1 s and ART = 3 s). For ART = 300 s and ART = 3000 s, the results show some resistance to black hole attacks. It can

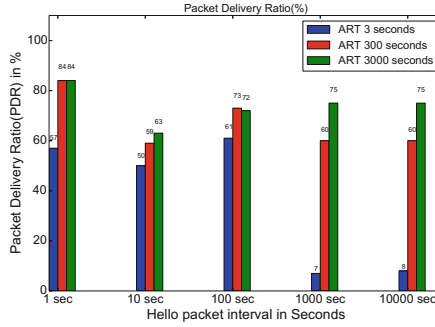


Fig. 4. Average packet delivery ratio with malicious activities

be seen that PDR is generally improved with the increase of ART in presence of malicious meters. This is because increasing the route lifetime can countermeasure a black hole attack. More specifically, the route discovery process is minimum when the ART value is larger and hence it shows resistance to black hole attacks to some degree. In addition, PDR changes with variation of Hello packet interval but this depends on a specific topology and meter polling frequency. In our case, PDR is maximized when ART = 3000 s and Hello packet interval = 1 s. In general, this simulation result suggests that higher PDR values could be achieved with a higher ART under a black hole attack.

#### 4.2 Effect of Variation of ART and Hello Packet Frequency on Average End-to-End Delay

In this subsection, we evaluate the impact of black hole attacks on end-to-end delay of the network. The average end-to-end delay is calculated from all normal senders with or without the malicious meter, based on the topology illustrated in Fig. 2. The results are plotted in Figs. 5 and 6 while changing the ART and Hello packet interval.

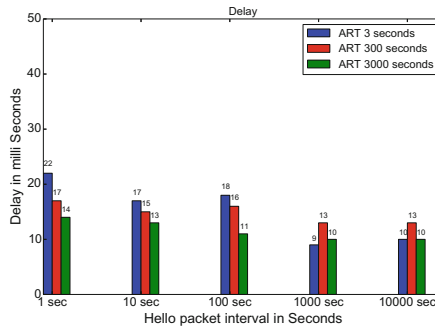
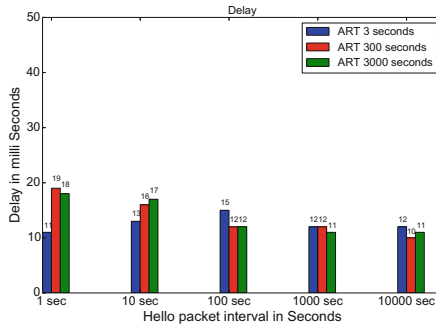


Fig. 5. Average delay without malicious activities



**Fig. 6.** Average delay with malicious activities

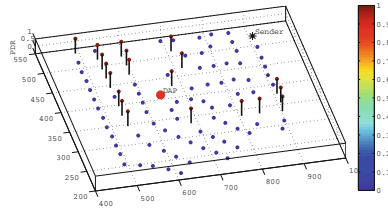
Without malicious meters, Fig. 5 demonstrates that a smaller ART usually results in a larger delay. It can be found that the average end-to-end delay decreases at a higher value of ART and Hello interval. For the default AODV setting (i.e., Hello packet interval = 1 s and ART = 3 s), the delay reaches 22 ms and is the largest one for all settings. This is because the meters frequently update the route state and the short Hello interval (i.e., 1 s) causes flooding the network every second, which ultimately results in the increase of delay. In general, this simulation result discovers that minimum delay can be achieved by increasing ART value since with a large ART, the meters will keep route states for a long time. In addition, the Hello packet interval can be tuned according to a specific topology to achieve a minimum delay. The appropriate Hello packet interval is 1000 s in our topology.

Figure 6 illustrates the average end-to-end delay with the malicious meter, whose position is marked in Fig. 2. The average delay in Fig. 6 is smaller than that observed in Fig. 5 due to that most of packets are dropped by the malicious meter and they fail to be transmitted to DAP. It is also shown that the average end-to-end delay decreases when Hello packet interval and ART are increased, which is similar to the trend in Fig. 5.

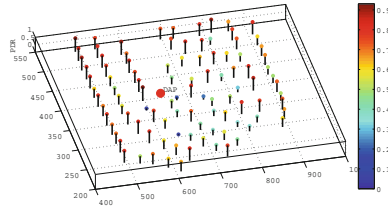
### 4.3 Effect of Position of Malicious Meters on PDR

In this subsection, we evaluate the PDR while changing the position of malicious meters in Fig. 2. Two different scenarios are considered: (1) only one specific source meter sends data to the DAP and (2) all meters take turn to send data to the DAP. In the first scenario, one specific sender is the attacking target, which is marked as “\*” and DAP is marked as “red dot” as shown in Fig. 7. Each time, assume there is only one malicious meter, and the sender’s PDRs are recorded by making all other smart meters as a malicious one in turn. The 3-D result for the first scenario is shown in Fig. 7, in which the z-axis represents the sender’s PDR when the meter at the position (x, y) is compromised. It is clearly seen that the PDR varies when attacker changes its location. By intuition, we expect a reduction of PDR when the malicious meters are physically close to the sender





**Fig. 7.** Effect of position of malicious meters on PDR for a specific sender (Color figure online)



**Fig. 8.** Effect of position of malicious nodes on PDR for overall senders

or the destination. Unfortunately, from this figure, there is no obvious trend to support that intuition. The PDR can still reach 0 even when the malicious meter is far away to both sender and DAP.

In the second scenario, one malicious meter is assumed and all other meters successively send data to the DAP. The average PDR is recorded for all regular meters when the malicious meter changes the position. The 3-D result for this scenario is shown in Fig. 8, in which the z-axis represents the average PDR when the meter at the position (x, y) is compromised while all other meters are good meters. It is observed that the average PDR also changes if malicious meter is placed at different locations, but no general trend is concluded.

## 5 Conclusions

In this paper, we have evaluated the black hole attack from new perspectives, by changing the AODV routing parameters including Hello message interval and rout lifetime as well as positions of malicious meters. Simulation results demonstrate that different AODV parameters will result in different performance. Hence parameter of AODV can be tuned according to a specific topology to achieve better performance. We have also studied the impact of the position of malicious meters on black hole attack. These findings will provide insights into security improvement in smart metering networks, e.g., malicious meters detection and robust routing protocol design.

## References

1. Utility-scale smart meter deployments: building block of the evolving power grid. IEI report (2014)
2. Erol-Kantarci, M., Mouftah, H.T.: Energy-efficient information and communication infrastructures in the smart grid: a survey on interactions and open issues. *IEEE Commun. Surv. Tutor.* **17**(1), 179–197 (2015)
3. Ho, Q.-D., Gao, Y., Le-Ngoc, T.: Challenges and research opportunities in wireless communication networks for smart grid. *IEEE Wirel. Commun.* **20**(3), 89–95 (2013)
4. Xu, J., Zhang, R.: CoMP meets smart grid: a new communication and energy cooperation paradigm. *IEEE Trans. Veh. Technol.* **64**(6), 2476–2488 (2015)
5. Bennett, C., Wicker, S.B.: Decreased time delay and security enhancement recommendations for AMI smart meter networks. In: *IEEE Innovative Smart Grid Technologies (ISGT)*, pp. 1–6 (2010)
6. Esmaili, H., Shoja, M., et al.: Performance analysis of AODV under black hole attack through use of OPNET simulator. *World Comput. Sci. Inf. Technol. J. (WCSIT)* **1**, 49–52 (2011)
7. Klein-Berndt, L.: A quick guide to AODV routing. In: *NIST, Wireless Communications Technologies Group* (2011). [http://w3.antd.nist.gov/wctg/aodv\\_kernel/](http://w3.antd.nist.gov/wctg/aodv_kernel/)
8. Gellert, W.: *The VNR Concise Encyclopedia of Mathematics*. Springer Science and Business Media, Heidelberg (2012)
9. Yi, P., Zhu, T., Zhang, Q., Wu, Y., Li, J.: A denial of service attack in advanced metering infrastructure network. In: *IEEE International Conference on Communications (ICC)*, pp. 1029–1034 (2014)
10. Wang, G., Ren, Y., Dou, K., Li, J.: IDTCP: an effective approach to mitigating the TCP incast problem in data center networks. *Inf. Syst. Front.* **16**, 35–44 (2014)
11. Wang, G., Ren, Y., Li, J.: An effective approach to alleviating the challenges of transmission control protocol. *IET Commun.* **8**(6), 860–869 (2014)
12. Al-Mandhari, W., Gyoda, K., Nakajima, N.: Performance evaluation of active route time-out parameter in ad-hoc on demand distance vector (AODV). In: *The 6th WSEAS International Conference on Applied Electromagnetic, Wireless and Optical Communications*, pp. 2–4 (2008)