UDC 621.391

EFFECTS OF WORMHOLE ATTACK ON ROUTING TOPOLOGY

J. KASHAIJA
Kharkiv National University of Radio Electronics

Abstract *– The article is devoted to investigating the effects of wormhole attacks on routing topology in Wireless Sensor Networks (WSNs). Currently, WSNs are increasingly vulnerable to numerous security attacks. One of the major attacks affecting WSNs involves a wormhole attack where attackers receive packets at a single end in the network and tunnel the packets to other points in the network and are subsequently replayed in the network. The wormhole attacks can affect the routing topology by redirecting traffic. Because of the nature of WNSs, attackers can develop a wormhole for packets not destined for them due to overhearing them within the wireless network and tunneling them to colluding attackers on the opposite side of the wormhole. Mainly, wormhole attacks are hazardous to ad-hoc network routing protocols. Therefore, it is evident that routing topology suffers from various vulnerabilities and needs robust security measures. This research investigates the effects of wormhole attacks on routing topology, and a simulation is presented to depict wormhole attack effects. In addition, an analysis of wormhole simulation of packet transmission with and without attacker node using Network Simulator NS-2 environment has been carried out. A simulation conducted using NS2 determined the performance of two reactive routing protocols (AODV and DSR) using their throughput, the first and the last packet received, and the total amount of bytes received in two conditions (with and without wormhole). Findings obtained demonstrate that the performance of DSR was better compared to that of AODV. The introduction of wormhole attacks in both routing protocols significantly affected the performance.*

Анотація *– Стаття присвячена дослідженню впливу Wormhole атаки на маршрутну топологію в безпроводових сенсорних мережах (Wireless Sensor Networks, WSN). Зараз мережі WSN стають дедалі вразливішими до численних атак безпеки. Однією з основних атак, що впливають на WSN, є Wormhole атака, коли зловмисники отримують пакети на одному кінці мережі та тунелюють пакети в інші точки мережі, а потім відтворюють у мережі. Wormhole атаки можуть впливати на топологію маршрутизації шляхом перенаправлення трафіку. Через властивості WSN зловмисники можуть створити Wormhole для пакетів, які їм не призначені, через те, що вони підслуховують їх у безпроводовій мережі та тунелюють їх зловмисникам, які змовляються з протилежного боку червоточини (Wormhole). В основному атаки через червоточину небезпечні для протоколів маршрутизації ad-hoc мереж. Таким чином, очевидно, що топологія маршрутизації страждає від різноманітних уразливостей і потребує надійних заходів безпеки. У цій роботі досліджується вплив атак через червоточину на топологію маршрутизації, а також представлено моделювання для зображення ефектів атак через червоточину. Крім того, було проведено аналіз моделювання передачі пакетів з атакуючим вузлом та без нього за допомогою середовища Network Simulator NS-2. Моделювання, проведене за допомогою NS2, визначило продуктивність двох реактивних протоколів маршрутизації (AODV і DSR), використовуючи їх пропускну здатність, перший та останній отриманий пакет і загальну кількість байтів, отриманих у двох умовах (з червоточиною та без неї). Отримані результати показують, що продуктивність DSR була кращою порівняно з AODV. Впровадження атак через червоточину в обох протоколах маршрутизації значно вплинуло на їхню продуктивність.*

Introduction

Breakthroughs witnessed in wireless communications have fostered the pervasive deployment of wireless sensor networks (WSNs). Attributed to their features, such as the easy deployment of sensor nodes, WSNs have been applied in various fields like rescue missions and monitoring environment conditions [1]. In [2], Kaur et al. noted that WSNs could also be used in monitoring physical conditions like temperature, pollutants, motion, vibration, sound, and pressure, as well as on battlefields, industrial monitoring, health monitoring, and controlling traffic. Their role is to provide critical information in real-time in monitoring and tracking applications [3]. Since such operations involve critical information, any vulnerability can be disastrous.

In WSNs, routing is applied to move data from the source to a given destination. Wormhole attacks can affect the routing topology by redirecting traffic. This research in-

vestigates the effects of wormhole attacks on routing topology, and a simulation is presented to depict wormhole attack effects.

I. Routing Topology

WSN routing is described as a process of transferring information from a given source to a chosen endpoint within an Ad-hoc network [4]. The process entails determining the ideal routing pathways and then moving information packets via an Ad-hoc network. The routing algorithms will decide the routes to be used by first sharing information amongst the immediate neighbors and subsequently in the entire network [5]. As a result, the routing protocols can gain knowledge of network topology. The routing mechanism usually considers the architecture and the software coupled with the features of the sensor nodes [6].

Various routing protocols are used to route data within WSNs: proactive, reactive, and hybrid [2-4, 7-10]. According to [2], reactive routing protocols create the pathways after the sources indicate that they need to send data to various destinations. Every node within the network will discover or maintain a route driven by on-demand. Reactive protocol flood control message by globally broadcasting when discovering route and when after discovering the routes, bandwidth is deployed to transmit data [5]. Their main benefit is that they require less touting information, but they generate massive control packets attributable to route discovery when topological changes occur. Also, reactive protocols experience significant latency. Examples of reactive protocols involve Associativity-Based Routing (ABR), Dynamic Source Routing (DSR), and Ad-hoc on Demand Routing (AODV). AODV does not regularly update the routing table [11]. AODV offers multicast and uncast broadcast, which involves the on-demand algorithm used to search for routes between various nodes. The protocol builds paths through route requests and route reply query cycles [12]. Another reactive protocol involves Dynamic Source Routing (DSR) intended for multihop wireless networks [13]. It enables networks to be entirely self-configuring and self-organizing devoid of using any network.

Conversely, proactive routing protocols usually employ a routing table. The routing tables are maintained by the routing protocol and are updated frequently [14]. Every node within the proactive protocol will broadcast messages to the whole network when the network topology changes. Nonetheless, proactive protocols are known to experience extra overhead costs attributable to updating information resulting in network throughput. Examples of proactive mechanisms involve Optimized link-state routing protocol (OLSR), and Distance Vector (DV), as well as Destination Sequenced Distance Vector (DSDV) [14].

Hybrid protocols incorporate reactive and proactive protocols while harnessing their best attributes [15]. Zone Routing Protocol (ZRP) encompasses a hybrid routing scheme that combines proactive and reactive routing approaches to address the challenges witnessed when proactive or reactive routing protocols are utilized separately. Authors of [16] asserted that ZRP integrates the best attributes of reactive and proactive techniques to

minimize control overheads in proactive routing, which can waste time in updating the routing tables and reduce the latency of discovering a route experienced in reactive routing.

II. Wormhole attacks on Routing Topology

WSNs are increasingly vulnerable to numerous security attacks. One of the major attacks affecting WSNs involves a wormhole attack where attackers receive packets at a single end in the network and tunnel the packets to other points in the network and are subsequently replayed in the network [17]. When the tunneled intervals are extended than a single hop's usual wireless transmission scope, it becomes easier for the malicious actors to compel tunneled packets to reach with superior metrics compared to the regular multihop route. Also, attackers can probably forward each bit over the wormhole straightforwardly, minus holding back for the whole packets to arrive before starting tunneling of bits of the packets to reduce delays [6]. Because of the nature of WNSs, attackers can develop a wormhole for packets not destined for them due to overhearing them within the wireless network and tunneling them to colluding attackers on the opposite side of the wormhole. Attackers conducting tunneling reliability and honorably will not cause any harm since they foster efficiency by providing meaningful services [18]. Nonetheless, wormhole attacks make malicious actors powerful compared to network nodes. Hence, attackers can exploit such a powerful stance in various ways.

Additionally, wormhole attacks can be undertaken even when the network communication offers authenticity and confidentiality and when the actors cannot access cryptographic keys [17]. Moreover, attackers are increasingly invisible at higher layers. The occurrence of a wormhole and two clouding attacks at two endpoints of the wormhole are invisible to the route. Mainly, wormhole attacks are hazardous to ad-hoc network routing protocols [17]. For instance, it can be deployed against on-demand routing protocols like AODV and DSR to tunnel every ROUTE REQUEST packet directly to the destination targeted nodes of the REQUEST. Subsequently, the attacks will prevent others routes from being discovered [4]. Some techniques attackers use to exploit wormhole attacks involve discarding instead of forwarding all data packets (leading to DoS attack), and selectively modifying or discarding specific data packets.

Wormhole attacks impact location-based wireless security, data aggregation, and networking routing [19]. A wormhole attack can disrupt routing operations even without prior information about the encryption techniques deployed. Kaur et al. in [2] classified wormhole attacks into three kinds based on their mechanisms:

a) attacks deploying out of band channel;

b) attacks using protocol distortion;

c) attacks employing packet relay.

A wormhole attack that deploys out of band passage places a high bandwidth between endpoints to provide a link for the two-ended wormhole [6]. Meanwhile, attacks employing packet relay comprise one or more adversarial nodes that create packet-relay

attacks whereby the malicious nodes will replay data packets between two nodes located at a distant location. As a result, they create fake neighbors. The third attack utilizes protocol distortion as the nodes attempt to appeal to the network traffic. Wormhole attacks do not need MAC protocol information and are immune to cryptographic methods [20]. Thus, it is very challenging to detect. The attack has a significant effect on WSNs, especially on the routing protocols.

III. Simulation and Findings

Network Simulator NS-2 environment was deployed (developed by the University of California Berkley) to run WS simulations [21]. The environment is commonly utilized for wireless and wired networks as an object-oriented, event-based, and discrete simulation model programmed in C++. The simulator comprises an OTcl interpreter on the front end and can be freely accessed [21]. The simulator is centered on the layered approach and consists of rich protocols. Two simulations were run:

i) without attacker node;

ii) with attacker node.

Table 1 underneath depicts the simulation parameters.

Table 1. Wormhole Simulation Parameters

Parameters	**Values**
Malicious Node	Wormhole
Area	1500mx1500m
Network Mobility	Random
Simulation time	1000 seconds
Routing Protocols	DSR & AODV
Quantity of nodes	25
Applications	CBR
Data Rates	64 kbps

Subsequently, the simulation findings are presented for the first and last packets received, the total bytes received, and throughput based on AODV and DSR routing protocol with or without a wormhole (Fig. 1 – Fig. 4).

Fig. 1 shows the *first packet* received with and without a wormhole. Without a wormhole, AODV received 24 bytes while DSR received 6 bytes. In contrast, AODV received 7 bytes and DSR 2 bytes with a wormhole.

The *last packet* received is shown in Fig. 2. Without the wormhole, 75 bytes were received for AODV and 89 bytes for DSR routing protocols. However, 30 bytes were recorded for AODV and 57 bytes for DSR routing protocols with a wormhole.

The simulation documented the *total bytes* received as illustrated in Fig. 3. From Fig. 3, it is evident that more bytes were received without wormhole for both AODV (42,000) and DSR (47,000) than with wormhole: AODV (12,000) and DSR (28,000).

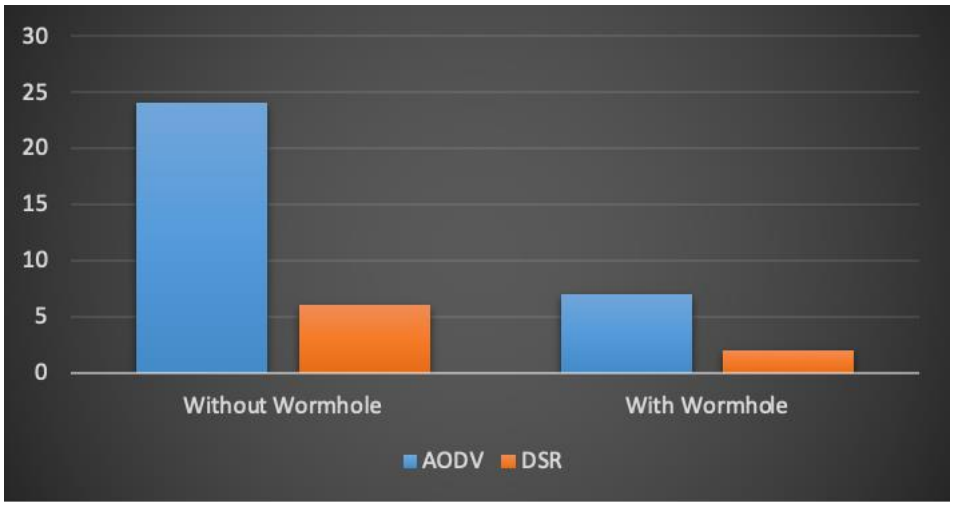

Fig. 1. The first packet received

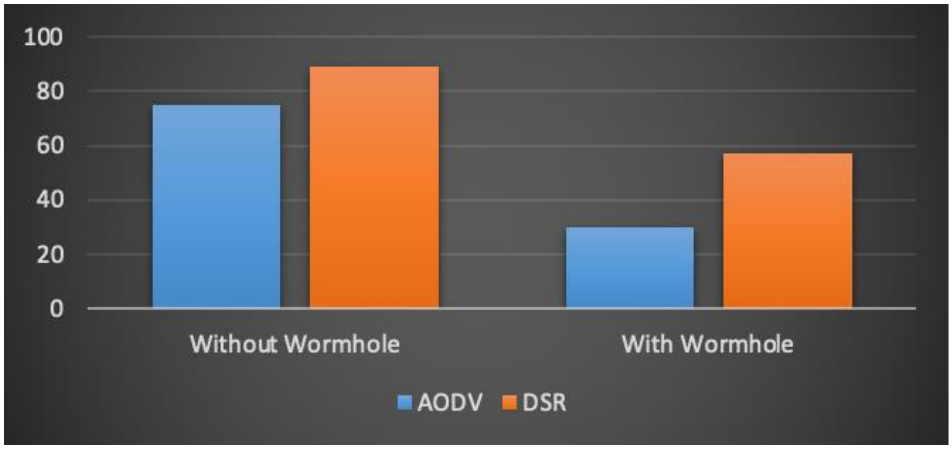

Fig. 2. The last packet received

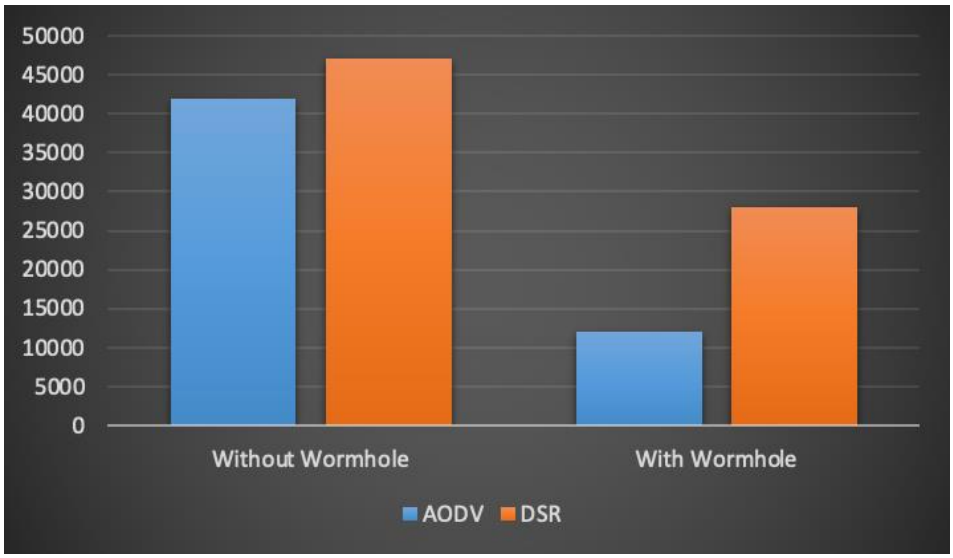

Fig. 3. Total bytes received

Also, the simulation examined the change in *throughput* (bits per second) with and without wormhole in both routing protocols. Fig. 4 indicates a higher throughput without a wormhole than with a wormhole.

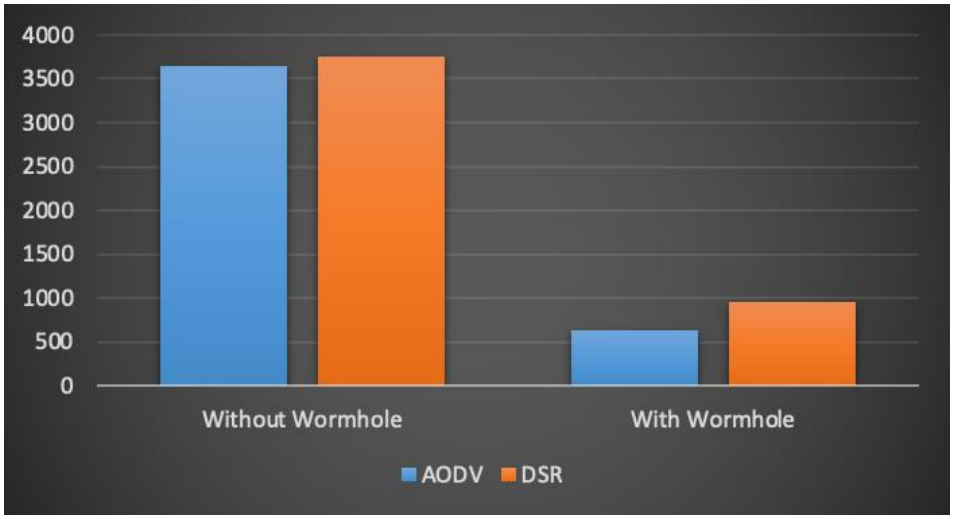

Fig. 4. Throughput

Conclusion

Wireless sensor network security remains a significant challenge as routing topology continues to be vulnerable to wormhole attacks. A simulation was conducted using NS2 to determine the performance of two reactive routing protocols (AODV and DSR) using their throughput, the first and the last packet received, and the total amount of bytes received in two conditions (with and without wormhole). Findings obtained demonstrate that the performance of DSR was better compared to that of AODV. The introduction of wormhole attacks in both routing protocols significantly affected the performance.

Therefore, it is evident that routing topology suffers from various vulnerabilities and needs robust security measures. Othmen et al. in [22] propose using the Anonymous on-demand Routing (ANODR) protocol to deliver net-centric anonymous and undetectable routing models for wireless ad-hoc networks. ANODR is centered on the table-driven AODV routing mechanism. It offers various security services: confidentiality and anonymity, identity-free routing, negligibility, one-time packet content, and confidentiality of traffic flows. Negligibility is centered on anti-tracing to ensure that signal interceptors will not track the movement trends of signal transmitters through wireless signal tracking. Anonymity is assured by ensuring that the path followed by the packets cannot be tracked by any malicious actor [22]. Also, the message content is concealed via encryption mechanisms to foster confidentiality. AODV ensures that the identity cannot be compromised or stolen by malicious users.

References

1. *Chen, H., Wu, H., Hu, J., Gao, C.* (2008), "Event-based trust framework model in wireless sensor networks", Proceedings of the 2008 International Conference on Networking, Architecture, and Storage, Chongqing, China, 12-14 June, P. 359-364. **DOI**: https://doi.org/10.1109/NAS.2008.33

2. *Kaur, G., Dhanda, E. S. K.* (2013), "Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, No. 2(8), P. 3230-3236.

3. *Ismail, M., Sanavullah, M. Y.* (2008), "Security topology in wireless sensor networks with routing optimisation", Proceedings of the 2008 Fourth International Conference on Wireless Communication and Sensor Networks, Indore, India, 27-29 December, P. 7-15. **DOI**: https://doi.org/10.1109/WCSN.2008.4772673

4. *Otmani, M., Ezzati, D. A.* (2014), "Effects Of Wormhole Attack On AODV And DSR Routing Protocol Through The Using NS2 Simulator", IOSR Journal of Computer Engineering (IOSR-JCE), No. 16(2), P. 101-107.

5. *Govindasamy, J., Punniakody, S.* (2018), "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack", Journal of Electrical Systems and Information Technology, No. 5(3), P. 735-744. **DOI**: https://doi.org/10.1016/j.jesit.2017.02.002

6. *Sakiz, F., Sen, S.* (2017), "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV", Ad Hoc Networks, No. 61, P. 33-50. DOI: https://doi.org/10.1016/j.adhoc.2017.03.006

7. *Лемешко, О. В., Єременко, О. С., Невзорова, О. С.* (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с. **DOI**: https://doi.org/10.30837/978-966-659-282-1

8. *Yeremenko, O. S., Ali, S. A.* (2015), "Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET", Radioelectronics and Informatics, No. 1(68), C. 26-29.

9. *Yeremenko, O., Lemeshko, O., Persikov, A.* (2018), "Secure Routing in Reliable Networks: Proactive and Reactive Approach", Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655. **DOI**: https://doi.org/10.1007/978-3-319-70581-1_44

10. *Yeremenko, O., Lemeshko, O., Persikov, A.* (2017), "Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in Communication Network", Proceedings of the 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 5-8 September, P. 87-90. **DOI**: https://doi.org/10.1109/STC-CSIT.2017.8098743

11. *Kamini, K., Kumar, R.* (2010), "VANET parameters and applications: A review", Global Journal of Computer Science and Technology, No. 10(7), P. 72-76.

12. *Maurya, P. K., Sharma, G., Sahu, V., Roberts, A., Srivastava, M., Scholar, M. T.* (2012), "An overview of AODV routing protocol", International Journal of Modern Engineering Research (IJMER), No. 2(3), P. 728-732.

13. *Cheng, Y., Cetinkaya, E. K., Sterbenz, J. P.* (2012), "Dynamic source routing (DSR) protocol implementation in ns-3", Proceedings of the 5th international ICST conference on simulation tools and techniques, P. 367-374.

14. *Shruthi, S.* (2017), "Proactive routing protocols for a MANET–A review", Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10-11 February, P. 821-827. **DOI**: https://doi.org/10.1109/I-SMAC.2017.8058294

15. *Safdar, V., Bashir, F., Hamid, Z., Afzal, H., Pyun, J. Y.* (2012), "A hybrid routing protocol for wireless sensor networks with mobile sinks", Proceedings of the ISWPC 2012 proceedings, P. 1-5. **DOI**: https://doi.org/10.1109/ISWPC.2012.6263665

16. *Raju, S. R., Mungara, J.* (2010), "Performance evaluation of zrp over aodv and dsr in mobile adhoc networks using qualnet", European Journal of Scientific Research, No. 45(4), P. 658-674.

17. *Dwivedi, S., Tripathi, P.* (2014), "An efficient approach for detection of wormhole attack in mobile ad-hoc network", International Journal of Computer Applications, No. 104(7), P. 18-23. **DOI**: https://doi.org/10.5120/18214-9172

18. *Fazeldehkordi, E., Amiri, I. S., Akanbi, O. A.* (2015), "A study of black hole attack solutions: On aodv routing protocol in manet, Syngress, 122 p.

19. *Jinwala, D.* (2006), "Ubiquitous computing: wireless sensor network deployment, models, security, threats and challenges", Proceedings of the National conference NCIIRP-2006, SRMIST, P. 1-8.

20. *El Kaissi, R. Z., Kayssi, A., Chehab, A., Dawy, Z.* (2005), "DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks", Proceedings of the The Second International Conference on Innovations in Information Technology (IIT'05), P. 1-10.

21. *Rehmani, M. H., Saleem, Y.* (2015), "Network simulator NS-2. In Encyclopedia of Information Science and Technology", Third Edition, P. 6249-6258.

22. *Othmen, S., Zarai, F., Belghith, A., Kamoun, L.* (2016), "Anonymous and secure on-demand routing protocol for multi-hop cellular networks", Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia, 11-13 May, P. 1-6. **DOI**: https://doi.org/10.1109/ISNCC.2016.7746093