UML Modeling of Cross-Layer Attack in Wireless Sensor Networks

Jian Wang[1(✉)], Abraham O. Fapojuwo[2], Chen Zhang[1], and Huiting Tan[1]

[1] School of Electronic Science and Engineering, National University of Defense Technology, Changsha, China
jwang@nudt.edu.cn
[2] Department of Electrical and Computer Engineering, University of Calgary, Calgary, Canada
fapojuwo@ucalgary.ca

Abstract. The openness of wireless communication and the unattended nature of sensor node deployment make it easy for an adversary to launch various attacks on wireless sensor networks. Cross-layer attack aims to achieve better attack effects, conceal attack behavior more better, reduce the cost of attack by using information from multiple protocol layers, or initiate attack at multiple layers cooperatively. There are now different understandings about cross-layer attack. In this paper, the definition of cross-layer attack is proposed and several cases of attacks are presented. In order to better understand their behaviors, the cases of cross-layer attack are modeled by utilizing unified modeling language, which helps to build more secure wireless sensor networks.

Keywords: Cross-layer attack · Unified modeling language · Wireless sensor networks

1 Introduction

Wireless sensor networks (WSNs) are growing enormously and widely used in a broad range of fields, such as industry, agriculture, city control, medical treatment and environmental monitoring. As one of the key elements of the Internet of Things, WSNs help to obtain information for the Internet of Things. WSNs are composed of a large number of micro and low-power and low-priced sensor nodes deployed in sensing fields. By the method of wireless communication, these sensor nodes form a self-organized, self-adapted, and multi-hopped intelligent network system and transmit sensed information to the processing center through the base station. Different from other wireless communication networks, the resources of WSNs nodes, such as computation, storage, communication and energy, are limited and the sensor nodes are commonly deployed in unattended areas where the battery can neither be replaced nor recharged.

In view of the limitation of the resources of sensor nodes, the high-strength security mechanisms cannot be implemented in WSNs. Due to the openness of the deployment of nodes, the sensor nodes might be captured by the attacker and the sensitive information might be leaked or compromised. Thus, WSNs are facing more serious security

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2017
N. Mitton et al. (Eds.): InterIoT 2016/SaSeIot 2016, LNICST 190, pp. 104–115, 2017.
DOI: 10.1007/978-3-319-52727-7_12

problems than the common traditional wireless networks, such as cellular networks. WSNs are susceptible to many different types of attacks at all layers of communication. An attacker can launch jamming [1] and tampering attacks [2, 3] at the physical layer. Attacks at the data link layer include collision [4], denial of sleep [5], Guaranteed Time Slot (GTS) attack [6], back-off manipulation [6] etc. The network layer of WSNs is vulnerable to different attacks, such as spoofed routing information [8], selective packet forwarding [8], sinkhole [8], wormhole [9], blackhole [10], sybil [11], hello flood [8], etc. Flooding attack and de-synchronization attack [1] are the attacks launched from the transport layer.

Besides the attacks directed to a single protocol layer, there are cross-layer attacks which relate to multiple layers in WSNs. Cross-layer attack can launch from one layer but aimed to another layer, use the information of one layer to produce an attack on another layer, or initiate at multiple layers cooperatively. The objectives of cross-layer attack are to achieve better attack effects, conceal attack behavior more better, or reduce the cost of attack. There are many different understandings about cross-layer attack [12–20]. In order to develop secure mechanism for WSNs, it is important to have a better understanding of cross-layer attack.

In this paper, cross-layer attacks in WSNs are studied at great depth. The main contributions of this paper are twofold. First, we propose a new definition of cross-layer attack and present several cases in different scenarios. Second, to better describe the behaviors of cross-layer attacks, we use Unified Modeling Language (UML) as the modeling framework.

The rest of this paper is organized as follows. Section 2 summarizes the related works about cross-layer attacks and propose a new definition of cross-layer attack. Section 3 presents the cases of cross-layer attack and its model. Finally, Sect. 4 concludes the paper.

2 Cross-Layer Attack in WSNs

The objectives of an attacker are to disrupt the security attributes of WSNs, including confidentiality, integrity, availability and authentication. To achieve these objectives, an adversary can launch attacks from different protocol layers of WSNs. At the physical layer, the adversary can jam the physical channel by interfering with the radio frequencies that nodes use for communication. Due to the unattended and distributed nature of deployment, the adversary can extract the secret information from the captured node, tamper with its circuitry, modify the program codes, or even replace it with malicious sensor [2, 3]. Data link layer is primarily responsible for medium access control, error control and frame detection. Attacks at the data link layer aim to disrupt the availability of the network by purposefully creating collisions, obtain unfair priority in the contention of channel or dissipate the limited energy of nodes. Network layer is primarily responsible for packet delivery including routing through intermediate nodes. Attacks at this layer aim to disrupt the network routing, acquire or control the data flows. Attacks at the transport layer aim to affect the data transmission by disrupting the existing connection or exhausting the connection resources. As described above,

an attacker can achieve different goals by launching attack from different protocol layers. Actually, the attacker may not just restrict his attack at one layer.

Some previous works have been done in the area of cross-layer attack in WSNs [12–20]. Radosavac et al. considered a kind of cross-layer attack which propagated from Medium Access Control (MAC) layer to routing layer, causing serious degradation of network performance [12]. In their scenario, an attacker utilizes legitimate communication patterns in MAC layer to isolate one or multiple nodes in the network and break existing paths in the routing layer. Thus, the attacker increases the probability of including himself in the new routes. Bian et al. described the Stasis Trap attack that is launched from the MAC layer but aims to degrade the end-to-end throughput of flows at the transport layer [13]. In this attack, the adversary periodically preempts the wireless channel by using a small Contention Window (CW) size in order to cause large variations in the Round Trip Time (RTT) of Transmission Control Protocol (TCP) flows. This in turn will cause the Retransmission Timeout (RTO) of the flows to expire and the congestion window size will be reduced to one and retransmit outstanding packets according to the congestion control mechanism. This chain of events will result in a significant drop in the throughput of flows. This kind of attack has very little effect on the MAC layer throughput and hence it is very hard to be detected at the MAC layer, but it can severely degrade end-to-end throughput. Nagireddygari and Thomas analyzed the MAC-TCP cross-layer attack in cognitive radio networks [14]. León et al. presented the Lion attack performed at the physical/link layer that affects the transport layer in cognitive radio networks [15]. This attack relies on specific jamming that forces frequent handoffs thus affecting the current TCP connections. Guang et al. presented shortcut attack and detour attack that originate at the MAC layer but aim to disrupt the performance of ad hoc routing mechanism [16]. Shao et al. discovered a cross-layer dropping attack against video steaming in Ad hoc networks [17]. An attacker can launch various packet dropping attacks at the network layer by exploiting the application layer knowledge without creating abnormal behavior. Panchenko et al. showed how application layer information can be used to speed up the attack on the network layer [18]. Wang et al. investigated the coordinated report false sensing attack (Physical layer) and small back-off window attack (MAC layer) in cognitive radio network and proposed a trust-based cross-layer defense framework [19]. Djahel et al. addressed a cross-layer attack targeting proactive routing protocols, which is launched at the routing level and reinforced at the MAC layer in order to amplify the resulting damage [20].

As described above, there are now different understandings about cross-layer attack. The attacks presented in [12–16], can be categorized as a kind of cross-layer attack which launches from one layer but aims to another layer. Obviously, there are associations between different layers of the network architecture and if an adversary launches an attack from one layer the performance of another layer is bound to be affected. However, in this kind of cross-layer attack, the effects on the layer at which the attack is initiated will be very limited, but it will have dramatic effects on the performance of another layer. Thus, it is not easy to detect the attack behavior at the layer, from which the attacker launches the attack. In [17, 18], the attacker can obtain information from one layer and then utilize it to initiate an attack at another layer. As a smart attacker, he can use the information acquired from different layers comprehensively and aim to achieve a better attack effects or conceal himself as far as possible.

In [19, 20], the adversary launched several attacks from different layers cooperatively in order to cause greater damage to the target. Wang et al. defined cross-layer attack as attack activities that are conducted coordinately in multiple network layers [19]. In our opinion, it is not necessary for cross-layer attack to enforce attack on multiple layers. An attack can also be categorized as cross-layer attack as long as it can create large effects on one layer through another layer. That is to say, for cross-layer attack, the adversary can initiate an attack at a single layer if he can achieve some special attack goals at multiple other layers. Different from the attacks against a single layer, by considering the situations of multiple layers cooperatively, cross-layer attack aims to reduce the probability of being detected, reduce the cost of attack or achieve the attack goals that may not be feasible by enforcing an attack on a single layer only. Based on the foregoing, we propose a new definition of cross-layer attack as

A cross-layer attack is a kind of attack that initiates at one protocol layer, or multiple protocol layers cooperatively, by considering vulnerabilities or information of multiple layers comprehensively, in order to achieve the attack goals that cannot be reached by only considering a single layer.

Actually, in the scenario of cross-layer attack that the attacker initiates attack at multiple layers, it is different from multi-layer attack. In multi-layer attack, the adversary should conduct attacks at multiple layers, however, it is not necessary that the attacks at different layers be cooperative, that is to say, they could be independent. For example, an attacker can execute Denial of Service (DOS) attack at the physical layer, MAC layer and network layer concurrently or alternately. If the attack on each layer is cooperative, it can be classified as cross-layer attack, otherwise it only belongs to multi-layer attack. In cross-layer attack, it is not necessary for the adversary to launch an attack from multiple layers. It can launch an attack from one layer but aimed to another layer and the attacks at different layers should be conducted cooperatively to achieve specific objectives. We will give some cases of cross-layer attack in WSNs in the following section.

3 Modeling of Cross-Layer Attacks

To defend cross-layer attack and design secure protocols in a WSN, it is important to understand the behaviors of cross-layer attack by building its behavioral model. The UML is a standard notation of real-world objects as a first step in developing an object-oriented design methodology. It is a language for specifying, visualizing, constructing, and documenting the artifacts and is used to evolve and derive the system. It presents a standard way to show interaction/behavior within the system. The UML provides a large set of diagrams, such as use case diagram, sequence diagram, activity diagram, state machine diagram, and deployment diagram to model the system behavior. We have selected the UML framework for modeling of cross-layer attacks because it provides security developers standardized methodologies for visualizing security attacks in WSNs. Some previous works have been done to describe the attacks at a single layer in WSNs using UML [21–23]. Uke et al. proposed behavioral modeling of physical and data link layer security attacks in WSNs using state machine diagram [21]. Pawar et al. presented behavioral modeling of WSNs MAC security

attacks using sequence diagram [22]. Hong et al. provided standard models for security attacks by UML sequence diagrams to describe and analyze possible attacks in the network and transport layers [23]. However, to the best of our knowledge, little research has been done in modeling of cross-layer attack in WSNs. In this section, we will present several cases of cross-layer attack in different scenarios and use UML to model them. These UML models will help security developers better understand the behaviors of cross-layer attack and the interaction of the system in presence of these attacks and build more secure WSNs.

3.1 MAC-Network Cross-Layer Attack

Attack at the MAC layer primarily aims to acquire priority in the contention of channel, dissipate the energy of the nodes, or create DOS. An attacker can cause collisions with neighboring nodes by sending jamming packets. And he can also get unfair priority access to the channel by setting a small CW value in the back-off mechanism, or modifying the Network Allocation Vector (NAV) in Request To Send (RTS) or Clear To Send (CTS) frames to reserve a longer time duration. At the network layer, an attacker can make himself a part of the routing path by sending bogus Route Reply (RREP) messages, advertising good Link Quality Indicator (LQI), such as low latency, low packet loss rate and small hop count.

In the scenario as described in Fig. 1(a), legitimate node A is the routing node and the data from other legitimate nodes, such as nodes B and C, are passed through it. A malicious node M wants to be the routing node in place of node A. It initiates attacks at the MAC and network layer coordinately to make himself being the node on the routing path (see Fig. 1(b)) and then it can launch selective forwarding, blackhole attack, etc. Actually, there are many kinds of attacks against MAC layer and network layer, we only give one example.

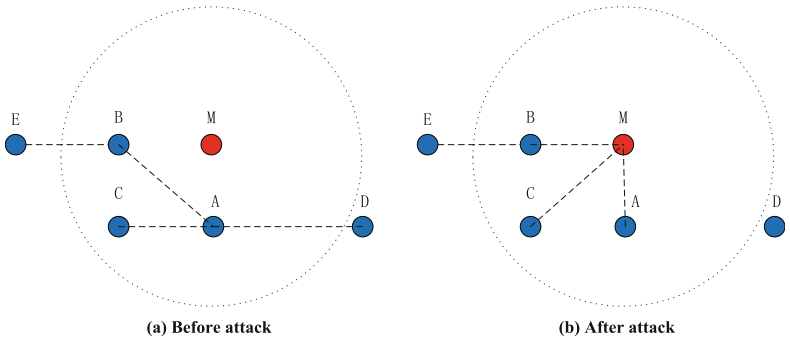

Fig. 1. Scenario of MAC-Network cross-layer attack

Figure 2 shows the flow of events in case of this kind of cross-layer attack. The detailed procedures are as follows.

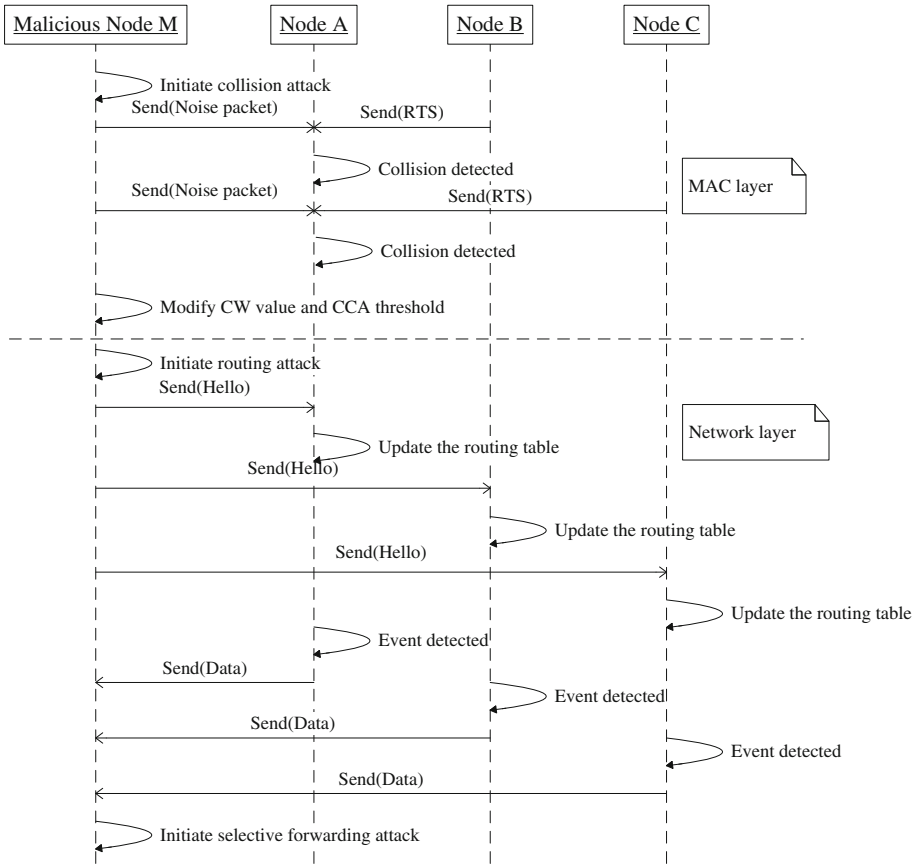

Fig. 2. Sequence diagram of MAC-Network cross-layer attack

(1) A malicious node M initiates collision attack on legitimate node A. When node B or C sends RTS to Node A, malicious node M generates a noise packet and sends it to node A at the same time. Both the packets will reach node A simultaneously and cause a collision. Thus, node B or C can hardly establish a channel with node A because the channel has been congested by malicious node M.

(2) Malicious node M modifies CW to a small value or increases its Clear Channel Assessment (CCA) threshold to a big value in order to acquire priority in the channel access.

(3) Malicious node M initiates routing attack by broadcasting bogus Hello message to the neighboring nodes. It advertises an attractive link quality for itself and the neighboring nodes take malicious node M as their new next hop routing node and update their routing Tables.

(4) The neighboring nodes detect the events and send their data to malicious node M. Thus, malicious node M can obtain the data of neighboring nodes and launch selective forwarding, blackhole attack, etc.

3.2 MAC-Transport Cross-Layer Attack

In Fig. 3, there are two end-to-end TCP flows, one is from node E to node C passing through node A, the other is from node F to node D passing through node B. Both nodes A and B are neighboring nodes of malicious node M.

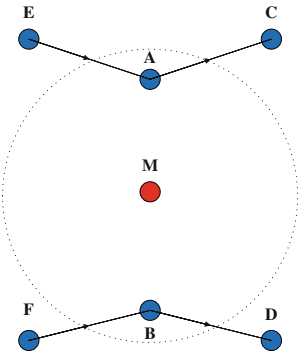

Fig. 3. Scenario of MAC-Transport cross-layer attack

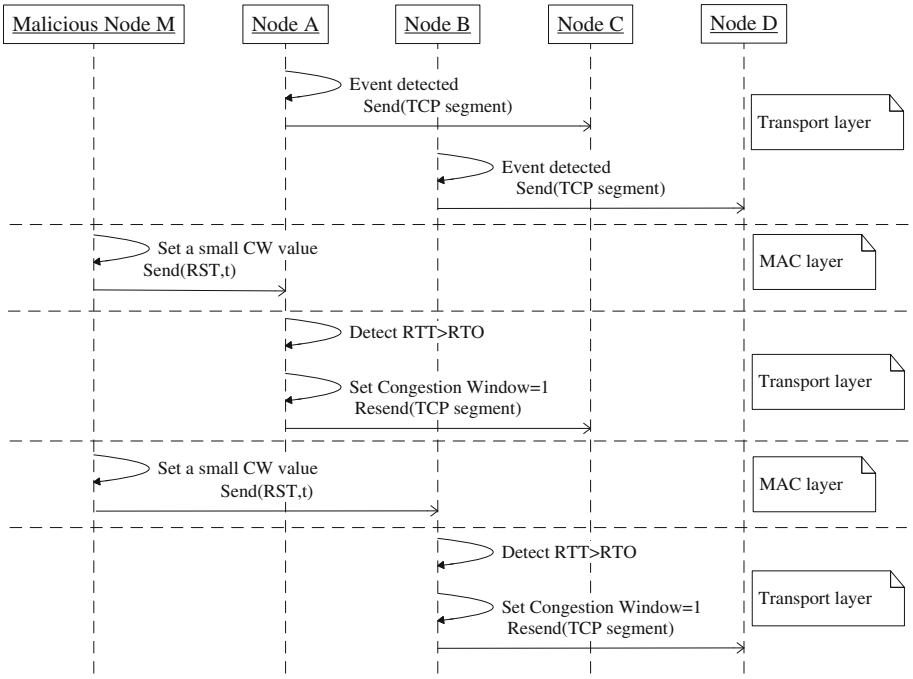

Fig. 4. Sequence diagram of MAC-Transport cross-layer attack

Malicious node M preempts the channel by manipulating the back-off mechanism at the MAC layer but its aim is to degrade the end-to-end throughput of flows at the transport layer [13]. Malicious node M manipulates the back-off values by using a small CW size and it can acquire the priority amongst all the contending nodes. Once the channel is preempted, malicious node M transmits data to node A or node B for a long enough period to cause noticeable delays in the TCP flows that are traversing through node A or B. According to the congestion control mechanism at the transport layer, if the RTT is delayed beyond the RTO, the congestion window size will be reduced to one and the outstanding packets will be retransmitted. Thus, the end-to-end throughput of the flows will be degraded seriously. Malicious node M preempts the channel periodically and switches transmission destination between node A and node B in a round-robin manner. It is very hard to detect the attack behavior at the MAC layer because it has very little effect on MAC layer throughput. The detailed procedures are as described in Fig. 4.

(1) Nodes A and B forward TCP segment to nodes C and D, respectively.
(2) Malicious node M sets a small CW size to acquire the priority in the contention of channel. It sends RTS frame to node A and the duration of occupying channel is t which is longer than the RTO.
(3) Node A detects that RTT is delayed beyond RTO and TCP sender will assume packet loss in this case. According to the congestion control mechanism, the congestion window value will be set to one and node A will retransmit the outstanding TCP segments.
(4) Malicious node M then switches the transmission destination to node B and performs the same operations on node B as it did to node A.
(5) Malicious node M periodically repeats the above steps (2)–(4).

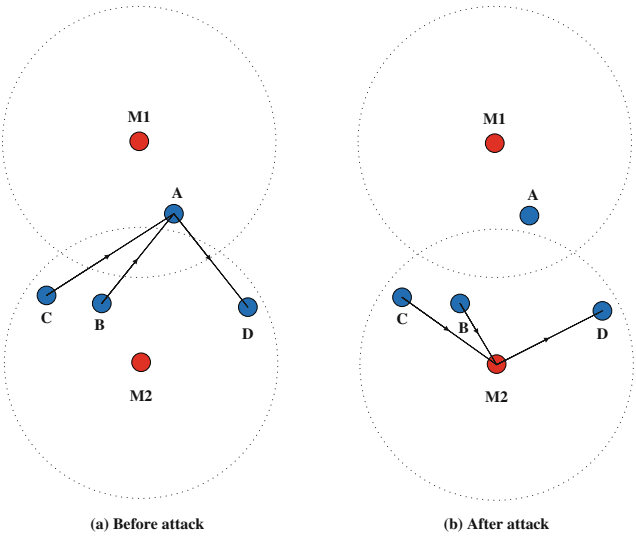

Fig. 5. Scenario of colluding cross-layer attack

3.3 Colluding Cross-Layer Attack

Figure 5 describes a scenario that two malicious nodes M1 and M2 collude to launch an attack. In this scenario, nodes B, C and D are neighboring nodes of node A. In Fig. 5 (a), node A is the next hop routing node of nodes B and C and it forwards the data of nodes B and C to node D. Node A is in the range of M1 and nodes B and C are in the range of M2. In order to disrupt the routing, malicious node M1 initiates collision attack on node A at the MAC layer and then malicious node M2 launches routing attack on nodes B and C at the network layer. After the attack, M2 becomes the next hop routing node of nodes B and C (see in Fig. 5(b)). Hence, M1 can initiate selective forwarding attack at the network layer.

The detailed procedures are as follows, illustrated in Fig. 6.

(1) Malicious node M1 intercepts the routing information sent by node A and acquires the information that node A is an important routing node.
(2) In order to disrupt the network routing, M1 performs collision attack on node A at the MAC layer. When other nodes send data to node A, M1 sends jamming packet

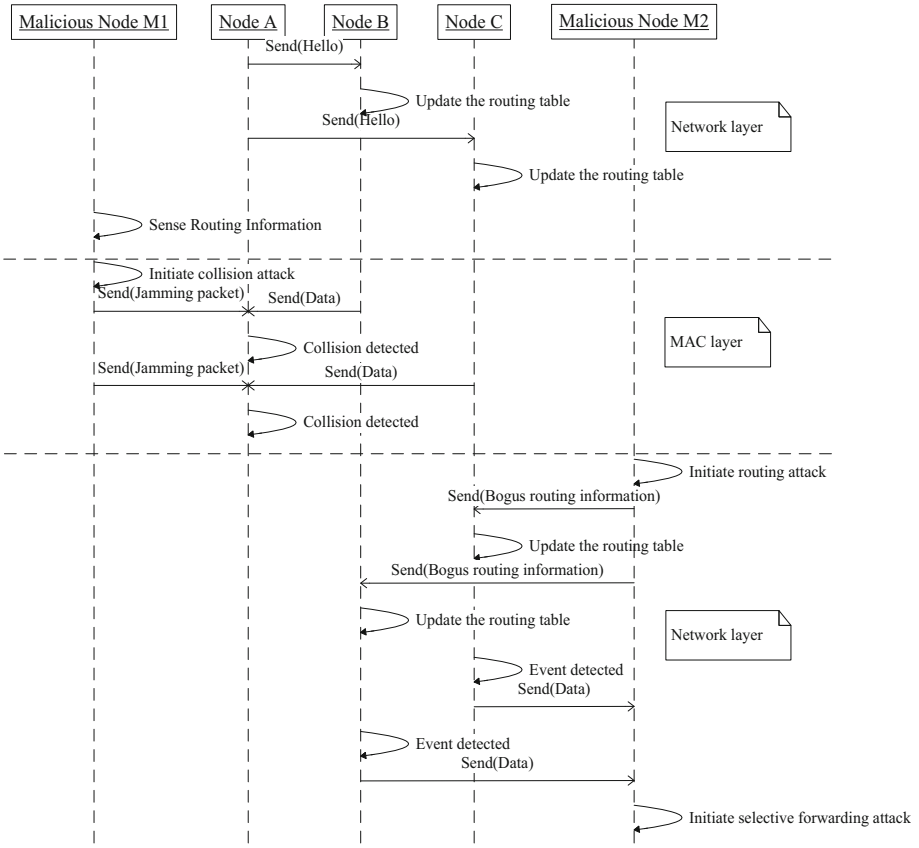

Fig. 6. Sequence diagram of colluding cross-layer attack

at the same time and then causes collisions. If the data transmission are always failed, nodes B and C may select another node as their next hop routing node.

(3) Malicious node M2 advertises a high quality route to node D to attract the traffic by sending bogus routing information. Then nodes B and C update their routing table. M2 becomes the next hop routing node of nodes B and C.

(4) Nodes B and C detect the event and send their data to M2, which then selectively forwards their packets to node D.

4 Conclusion

To conceal attack behavior more better, in cross-layer attack, it usually has little effects on the parameters of one protocol layer. Thus, for intrusion detection system, it can hardly distinguish normal behavior from abnormal behavior at one protocol layer because the deviation of protocol parameter is very small under cross-layer attack. And even if the intrusion detection system observes the anomaly, it is not easy to decide at which layer that the attack initiated and hence hard to make a response. For example, the modification of CW value will not bring huge effects to the contention of channel at the MAC layer and small changes in routing information will not draw more attention by the monitoring node. A smart attacker then utilizes MAC-Network cross-layer attack to achieve better attack effects on WSNs and decreases the probability of being detected at a single protocol layer as far as possible.

To detect cross-layer attack, it is necessary to use cross-layer based detection approach. Detection system monitors the critical parameters of multiple layers, such as Received Signal Strength Indication, Energy Reduction Rate at the physical layer, Back-off Time, Packet Collision Rate at the data link layer, Link Quality Indicator, Hop Count at the network layer, Number of Connections, RTT at the transport layer, Type of Data at the application layer. It draws a conclusion whether there is an attack behavior by analyzing the deviation of the parameters of different layers cooperatively. That is to say, detection system should not only extract features from multiple layers but also consider the correlation between attacks in different layers.

Wireless sensor networks are vulnerable to many types of attacks at different protocol layers due to the openness of the wireless channel and deployment of sensor nodes in an unattended area. Different from the attacks just aiming at a single layer, in cross-layer attack, an attacker can utilize the information from different layers separately or initiate attack at different layers cooperatively, and then achieve the attack goal that cannot be reached by only considering a single layer. Different explanations about cross-layer attack in WSNs currently exist. In this paper, we tried to study the objectives and behaviors of cross-layer attack and presented the definition of cross-layer attack. In order to better understand the behavior of cross-layer attack, we put forward several cases of cross-layer attacks and utilized sequence diagram to model them. These sequence diagrams show the attack's behaviors and the interactions between different objects in a network, which will be beneficial for developing secure solutions for WSNs. It is interesting to use other diagrams, such as activity diagram, state machine diagram, to model cross-layer attack in the future. The objective of

investigating attack's behaviors is to detect them. In future works, we will focus on how to design the structure of detection system in WSNs, how to deploy it and how to design effective cross-layer attack detection algorithms.

References

1. Wood, A.D., Stankvic, J.A.: Denial of service in sensor networks. IEEE Comput. **35**(10), 54–62 (2002)
2. Wang, X., Gu, W., Schosek, K., Chellappan, S., Xuan, D.: Sensor network configuration under physical attacks. Technical Report:OSU-CISRC-7/04-TR45, Department of Computer Science and Engineering, Ohio State University (2004)
3. Katsaiti, M., Rigas, A., Tzemos, I., Sklavos, N.: Real-world attacks toward circuits and systems design, targeting safety invasion. In: Proceedings of the 4th International Conference on Modern Circuits and System Technologies (MOCAST) (2015)
4. Xu, W., Ma, K., Trappe, W., Zhang, Y.: Jamming sensor networks: attack and defense strategies. IEEE Netw. **20**(3), 41–47 (2006)
5. Raymond, D.R., Marchany, R.C., Brownfield, M.I., Midkiff, S.F.: Effects of Denial-of sleep attacks on wireless sensor network MAC protocols. IEEE Trans. Veh. Technol. **58**(1), 367–380 (2009)
6. Sokullu, R., Dagdeviren, O., Korkmaz, I.: On the IEEE 802.15.4 MAC layer attacks: GTS attack. In: Proceedings of the Second International Conference on Sensor Technologies and Applications (SENSORCOMM), pp. 673–678 (2008)
7. Radosavac, S., Crdenas, A.A., Baras, J.S., Moustakides, G.V.: Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: robust strategies against individual and colluding attackers. J. Comput. Secur. **15**(1), 103–128 (2007). Special Issue on Security of Ad Hoc and SensorNetworks
8. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw. J. **1**(2–3), 293–315 (2003)
9. Hu, Y.C., Perrig, A., Johnson, D.B.: Packet Leashes: a defense against wormhole attacks in wireless networks. In: Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM), vol. 3, pp. 1976–1986 (2003)
10. Al-Shurman, M., Yoo, S.M., Park, S.: Black hole attack in mobile Ad hoc networks. In: Proceedings of the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42) (2004)
11. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: analysis & defenses. In: Proceedings of the Third International Symposium on Information Processing in Sensor Networks ACM (IPSN), pp. 259–268 (2004)
12. Radosavac, S., Benammar, N., Baras, J.S.: Cross-layer attacks in wireless ad hoc networks. In: Proceedings of the 38th Annual Conference on Information Science and Systems (CISS). Princeton University (2004)
13. Bian, K., Park, J.M., Chen, R.: Stasis Trap: cross-layer stealthy attack in wireless Ad hoc networks. In: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM) (2006)
14. Nagireddygari, D., Thomas, J.: MAC-TCP cross-layer attack and its defense in cognitive radio networks. In Proceedings of the 10th ACM International Symposium on QOS and Security for Wireless and Mobile Networks (Q2SWinet) (2014)

15. León, O., Hernández-Serrano, J., Soriano, M.: A new cross-layer attack to TCP in cognitive radio network. In: Proceedings of the Second International Workshop on Cross layer Design (IWCLD) (2009)
16. Guang, L., Assi, C., Benslimane, A.: Interlayer attacks in mobile Ad hoc networks. In: Cao, J., Stojmenovic, I., Jia, X., Das, Sajal, K. (eds.) MSN 2006. LNCS, vol. 4325, pp. 436–448. Springer, Heidelberg (2006). doi:10.1007/11943952_37
17. Shao, M., Zhu, S., Cao, G., Porta, T.L., Mohapatra, P.: A cross-layer dropping attack in video streaming over Ad hoc networks. In: Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (SECURECOMM) (2008)
18. Panchenko, A., Pimenidis, L.: Cross-layer attack on anonymizing networks. In: Proceedings of the 15th International Conference on Telecommunication (ICT) (2008)
19. Wang, W., Sun, Y., Li, H., Han, Z.: Cross-layer attack and defense in cognitive radio networks. In: Proceedings of IEEE Global Telecommunication Conference (GLOBECOM) (2010)
20. Djahel, S., Abdesselam, F.N., Khokhar, A.: A cross layer framework to mitigate a joint MAC and routing attack in multihop wireless network. In: Proceedings of the 5th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNET) (2009)
21. Uke, S.N., Mahajan, A.R., Thool, R.C.: UML modeling of physical and data link layer security attacks in WSN. Int. J. Comput. Appl. **70**(11), 25–28 (2013)
22. Pawar, P.M., Nielsen, R.H., Prasad, N.R., Ohmori, S., Prasad, R.: Behavioral modeling of WSN MAC layer security attacks: a sequential UML approach. J. Cyber Secur. Mob. **1**(1), 65–82 (2012)
23. Hong, S., Lim, S.: Analysis of attack models via unified modeling language in wireless sensor networks: a survey study. In: Proceedings of IEEE International Conference on Wireless Communications, Networking and Information Security (WCINS) (2010)