Behavioral Modeling of WSN MAC Layer Security Attacks: A Sequential UML Approach

Pawar, Pranav M.; Nielsen, Rasmus Hjorth; Prasad, Neeli R.; Ohmori, Shingo; Prasad, Ramjee

Published in:
Journal of Cyber Security and Mobility

Publication date:
2012

Document Version
Early version, also known as pre-print

Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach

Pranav M. Pawar[1], Rasmus H. Nielsen[2], Neeli R. Prasad[2], Shingo Ohmori[3] and Ramjee Prasad[1]

Center for TeleInFrastruktur, Aalborg University
[1]*Aalborg, Denmark*
[2]*Princeton, USA*
[3]*Yokosuka, Japan;*
e-mail: {in_pmp, rhn, np}@es.aau.dk, shingo_o@yiai.jp, prasad@es.aau.dk

Abstract

Wireless sensor networks (WSNs) are growing enormously and becoming increasingly attractive for a variety of application areas such as tele-health monitoring, industry monitoring, home automation and many more. The primary weakness shared by all wireless application and technologies is the vulnerability to security attacks/threats. The performance and behaviour of a WSN are vastly affected by such attacks. In order to be able to better address the vulnerabilities of WSNs in terms of security, it is important to understand the behaviour of the attacks.

This paper addresses the behavioural modelling of medium access control (MAC) security attacks in WSNs. The MAC layer is responsible for energy consumption, delay and channel utilization of the network and attacks on this layer can introduce significant degradation of the individual sensor nodes due

Journal of Cyber Security and Mobility, 65–82.

to energy drain and in performance due to delays. The behavioural modelling of attacks will be beneficial for designing efficient and secure MAC layer protocols. The security attacks are modelled using a sequential diagram approach of Unified Modelling Language (UML). Further, a new attack definition, specific to hybrid MAC mechanisms, is proposed.

Keywords: wireless sensor networks (WSNs), media access control (MAC), unified modelling language (UML), security and attacks.

1 Introduction

A WSN consists of a number of small nodes, equipped with sensors, which together form a network that can perform tasks by communicating with each other using a radio. WSNs have been used in many applications such as tele-health monitoring, intelligent transportation, industry monitoring, home automation and so on. Potentially, many of these WSN applications carry sensitive information, therefore to protect applications from different kind of denial of service attacks such as denial of sleep, collision attacks, exhaustion attacks and jamming attacks is a prime concern.

As compared with traditional network security, security in WSNs is more complex mainly due to computational constrains of the nodes and the objective to conserve energy in order to maximize the lifetime of the network and the individual nodes. The unpredictable communication channel and unattended operation make security in WSN seven harder [1].

A WSN network is susceptible to many different security attacks at all layers of communication and these attacks can introduce a large amount of inconsistencies in the network. In order to address attacks in a WSN through development of good security mechanisms, it is important to understand the behaviour of the attacks [2].

The MAC layer plays a central part in the operation of a WSN where it is responsible for determining energy consumption, channel capacity utilization and network delay [3]. These responsibilities of the MAC layer makes it vulnerable to many different attacks such as collision attacks, denial of sleep attacks, exhaustion attacks, etc. These attacks introduce large delays and increase the energy drain in the individual sensor nodes. Current research

in WSN security has focused less on security on the MAC security. However, understanding the behaviour of MAC security attacks is important in order to develop secure mechanisms for the MAC layer. The aim of this paper is to understand and model the behaviour of WSN MAC security attacks for development of efficient MAC mechanisms.

The UML based approach has been chosen for better analysis of security attacks behaviour [4, 5]. UML is a well-known modelling methodology and is a standard notation of real-world objects as a first step in developing an object-oriented design methodology. It is used as the language for specifying, visualizing and constructing the artefacts of the system. UML represents a collection of the best engineering practices that have proven successful in the modelling of large and complex systems. The important benefit of UML is that it provides security developers standardized methodologies for visualizing security attacks that are present in WSNs. Little research has been done in UML modelling of a WSN environment especially concerning the security.

This paper proposes behavioural modelling of WSN MAC security attacks using sequence diagrams. It shows the interaction between different objects in a network. It will be advantageous to develop competent secure MAC [6].

Further, the paper proposes a new attack definition named the Explicit Contention Notification (ECN) attack for hybrid MAC mechanisms. This attack can take place in hybrid MAC mechanisms such as Z-MAC [7], in which the malicious node will transmit the false ECN messages and increase the energy drain and delays in the WSN.

The remainder of this paper is organized as follows: Section 2 gives an overview of MAC layer security and different attacks. Section 3 presents the behavioural modelling of WSN MAC security attacks. Section 4 gives the details of the proposed attack and Section 5 concludes the paper.

2 MAC Layer Security and Attacks

Most of the research in WSN security has concentrated on the confidentiality and integrity of the data in the network. Due to the limited energy of a WSN, it remains extremely vulnerable to security attacks draining this, the most critical resource. The MAC protocol is responsible for managing the radio of sensor, which is the main source of power consumption. To design a secure MAC layer it is crucial to understand the normal and malicious sources of energy loss, which is essential to design the power control system.

Different security attacks, which amplify the energy drains and delays, can majorly affect the performance of the MAC layer. The effect of these attacks on the MAC layer performance can be minimized or removed, if the behaviour of the attacks is analysed and modelled. It enlightens the sequence of activities perform by attacker or malicious node. The following subsections explain the main MAC security attacks in detail.

2.1 Collision Attack

The malicious collision attack [8, 9] can be easily launched by a compromised sensor node. In a collision attack, a malicious node does not follow the MAC protocol rules and causes collisions with neighbouring nodes' transmissions by sending a short noise packet. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the network operation. It is difficult to detect this attack because of the broadcast nature of the wireless environment.

2.2 Unintelligent Replay Attack

In case of the unintelligent replay attack [10], the attacker does not have MAC protocol knowledge and no ability to penetrate the network. Here, recorded events are replayed into the network which prevent nodes from entering sleep mode and lead to waste in energy in receiving and processing the extra packets. If nodes are not equipped with an anti-replay mechanism this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination. The replaying of events has adverse effect on the network lifetime and overall performance of WSN.

2.3 Unauthenticated Broadcast Attack

In an unauthenticated broadcast attack [10], the attacker has full knowledge of the MAC protocol but does not have the capability to penetrate the network. Here, the attacker broadcasts the unauthenticated traffic into the network by following all MAC rules. These unauthenticated and unnecessary broadcast messages are disturbing the normal sleep and listen cycle of the node and place most of the nodes in listen mode for an extended amount of time; it leads to increase in energy consumption and reduction in network lifetime. These

attacks cause server harm to MAC protocols that are having short messages and short adaptive timeout period.

2.4 Full Domination Attack

Here, the attacker has full knowledge of the MAC layer protocol and ability to penetrate the network. This type of attack is one of the most destructive to a WSN as the attacker has the ability to produce trusted traffic to gain the maximum possible impact from denial of sleep. The attacks are mounted using one or more compromised nodes in the network. All kinds of MAC layer protocols are vulnerable to this kind of attack [10].

2.5 Exhaustion Attack

The attacker who commences an exhaustion attack [10] has knowledge about the MAC protocol and the ability to penetrate the network. These attacks are possible only in case of request to send (RTS)/clear to send (CTS) based MAC protocols. In this attack, the malicious node sends RTS to a node and if the node replies with CTS, the malicious node will repeatedly transmit the RTS to the node, which will prevent the node from going into sleep mode and instead drain the total energy of the node. These attacks are affecting the node lifetime and can partition the network.

2.6 Intelligent Jamming Attack

The intelligent jamming attack is one of the most disastrous attacks where attacker has full protocol knowledge but does not have the ability to penetrate the network. The attacker injects unauthenticated unicast and broadcast packets into the network. These attacks can differentiate between control traffic and data traffic and unlike the unauthenticated replay attack it replays the selective events (control or data) [10, 11].

3 Behavioural Modelling of MAC Security Attacks

3.1 UML Modelling

UML [5] is a language for specifying, visualizing, constructing, and documenting the artefacts and is used to evolve and derive the system. It presents a

standard way to show interactions/behaviour within the system that provides a conceptual understanding of system functionality.The UML provides a large set of diagrams such as use case diagram, sequence diagram, activity diagram, state machine diagram, deployment diagrams and many more to model the system behaviour.

The focus of this paper is to use UML to model security attacks using sequence diagrams [5]. The sequence diagram is used primarily to show the interactions between objects in the sequential order in which they occur also known as message sequence charts. A sequence diagram shows, as parallel vertical lines, different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. Here, the different nodes in the network and the external attacker are considered as objects and the interactions of the nodes after initiation of the attack are shown.

3.2 Modelling of Security Attacks

3.2.1 Collision attack

Figure 1 explains the flow of events in case of collision attacks. The details of each event are as follows:

- An external attacker initiates the collision attack through the malicious node 3.
- Once the attack is initiated on node 3, it will start to send noise packets to all nodes in the network. It will increase the traffic in the network causing the channel to become busy doing this activity.
- Node 1 detects an event and sends a RTS packet to node 2. At the same time the malicious node 3 also generates a noise packet and forwards it towards node 2. Both packets will reach node 2 simultaneously and cause a collision.
- Again, node 1 detects the event and checks channel availability by exchanging RTS and CTS with node 2. Once node 1 receives the CTS from node 2, node 1 starts to send data packets towards node 2. If, at the same time, the malicious node 3 also sends noise packets toward node 2, collisions will happen in the network.
- The malicious node 3 is continuously generating noise packets that make the channel constantly busy. During this, if any other node

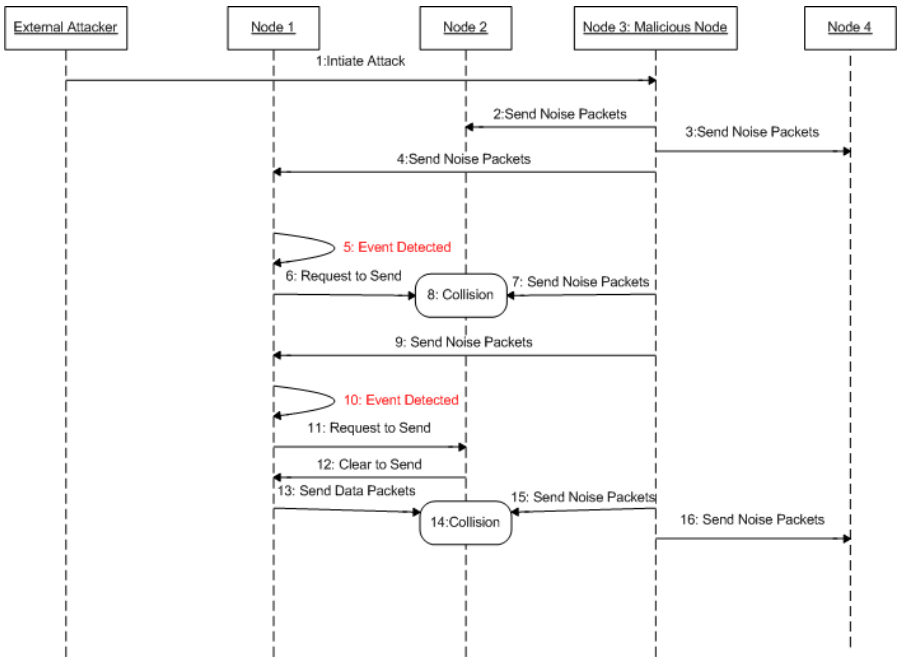

Figure 1 Sequence diagram of collision attack.

tries to use the channel, a collision will take place. This collision of packets leads to retransmission of the packets that in turn leads to increasing energy consumption.

3.2.2 Unintelligent replay attack

Figure 2 explains the flow of events in case of an unintelligent replay attack. The details of each event areas follow:

- An external attacker initiates the unintelligent replay attack through the malicious node 4.
- The malicious node 4 detects the event and sends an unauthenticated data/control packet towards the sink hop by hop, node 4 ->node 3 -> node 2 -> node 1.
- After some time, the malicious node 4 will replay the event and will forward it through the network. Here, the malicious node does not differentiate between control and data packets.

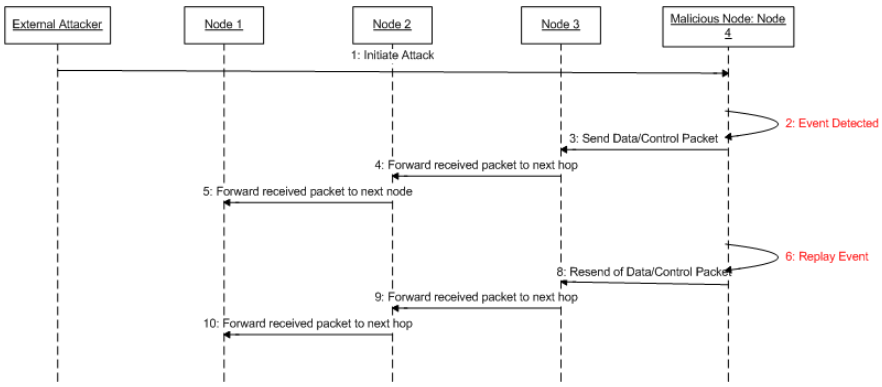

Figure 2 Sequence diagram of unintelligent replay attack.

- The event will be replayed again and again which increases the traffic in the network and prevents the nodes from going into sleep mode. An increasing number of nodes will be in listen mode, maximizing the power consumption at each node on the path to the destination. During this, if any other node tries to send a packet, it will get channel busy.

3.2.3 Unauthenticated broadcast attack

Figure 3 explains the flow of events in case of the unauthenticated broadcast attack. The details of each event are as follows:

- An external attacker initiates an unauthenticated broadcast attack through themalicious node 3.
- The malicious node 3 detects the event and broadcasts packet to the whole network.
- Whenever the packet reaches anode, the node will try to authenticate it but authentication will fail because, even though, in this attack, the attacker has full protocol knowledge, it does not have the ability to penetrate the network.
- Every time the malicious node 3 detects the event and broadcasts the packet to the whole network. This unnecessary broadcasting of packets will waste energy in all nodes in the network because nodes will have to wake up to listen due to the event.

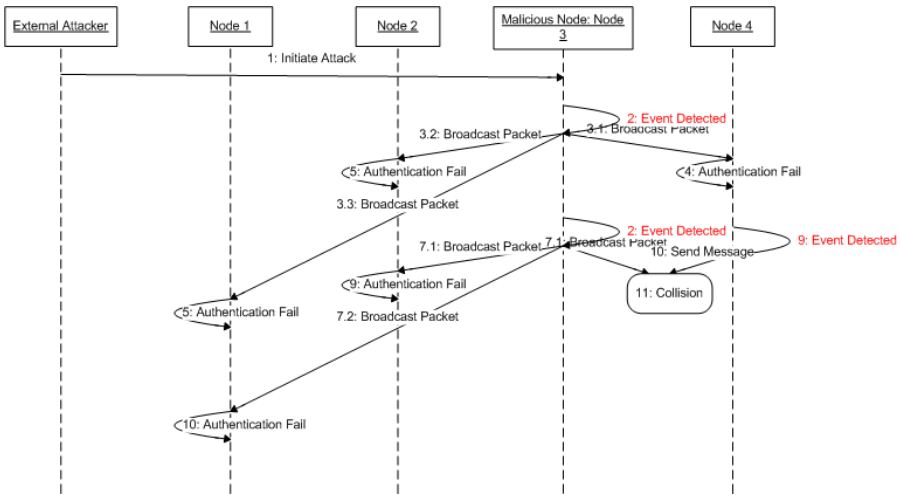

Figure 3 Sequence diagram of unauthorised broadcast attack.

- Node 4 detects the event and sends the message towards node 3. If, at the same time, the malicious node 3 detects and broadcasts the event, it leads to a collision on the channel between node 3 and node 4.

3.2.4 Full domination attack

Figure 4 explains the flow of events in case of full domination attack. The details of each event areas follow:

- An external attacker initiates the full domination attack through the malicious nodes 2 and 4.
- The malicious node 4 detects the event and broadcasts the message to the network. Here, the message is accepted by all nodes because, in this attack, the attacker has full knowledge of the MAC protocol and the ability to penetrate the network.
- The malicious node 2 detects the event and broadcasts the message to the network.
- The malicious node 2 replays the event again after some time and broadcasts it to whole network. The repeated broadcasting of the

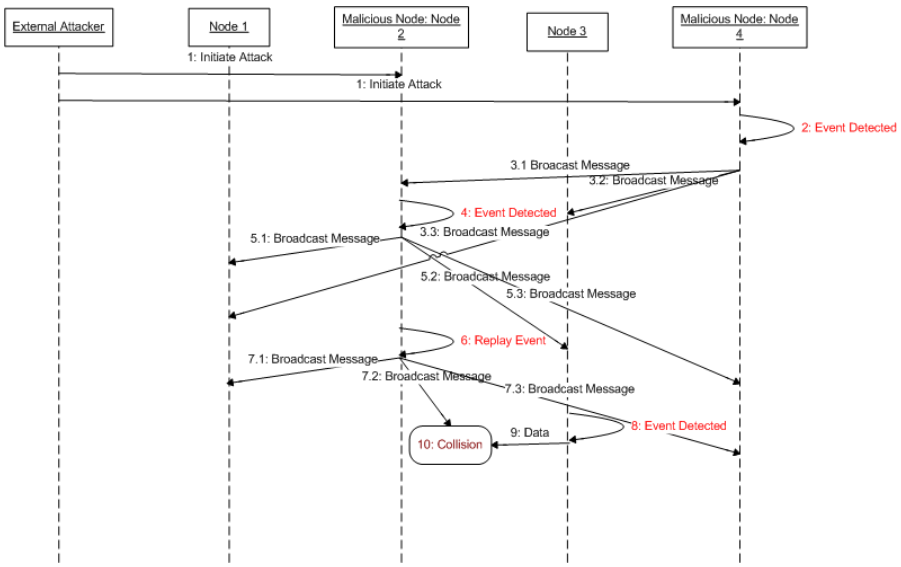

Figure 4 Sequence diagram of full domination attack.

event will prevent nodes from going into sleep mode, thus increasing the overall power consumption.

- Node 3 detects an event and sends the data and this collides with the broadcast message sent by the malicious node 2.

3.2.5 Exhaustion attack

Figure 5 explains the flow of events in case of the exhaustion attack. The details of each event are as follows:

- An external attacker initiates an exhaustion attack through the malicious node 4.
- Node 1 detects the event and exchanges RTS and CTS and finally sends the data to node 2.
- The malicious node 4 detects an event and sends RTS to node 2. Node 2 will reply by CTS. After that, the malicious node will repeatedly generate a RTS packet and transmit it towards node 2 until the total energy of node 2 is exhausted.

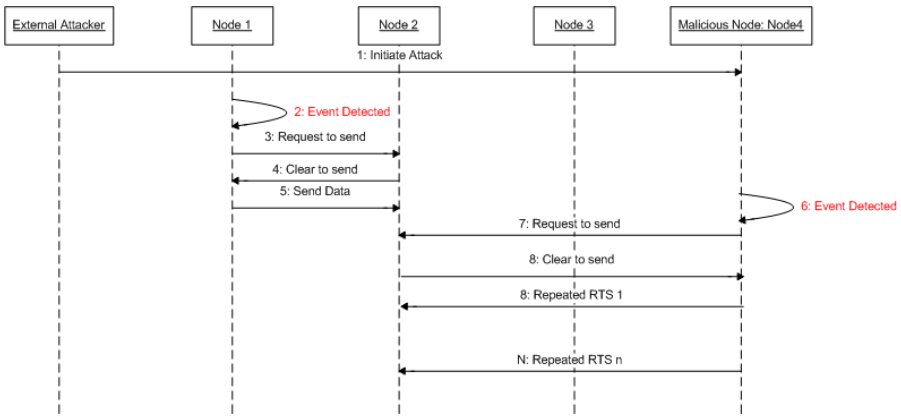

Figure 5 Sequence diagram of exhaustion attack.

3.2.6 Intelligent jamming attack

Figure 6 explains the flow of events in case of intelligent jamming attack. The details of each event areas follow:

- An external attacker initiates an intelligent jamming attack through the malicious node 4.
- The malicious node 4 detects the control event and transmits the unauthenticated unicast message to node 3.
- Node 3 detects an event and forwards the message towards node 1, this message collides with the message broadcasted by the malicious node 4.
- The malicious node 4 detects an event and broadcasts the unauthenticated broadcast message in the network.
- The malicious node 4 uses the knowledge of the MAC layer protocol for selective replay of data or control events. Node 4 replays the previously detected data event and transmits the unauthenticated unicast message to node 2.
- The malicious node 4 selectively replays the control event and broadcasts the unauthenticated control message in the network.

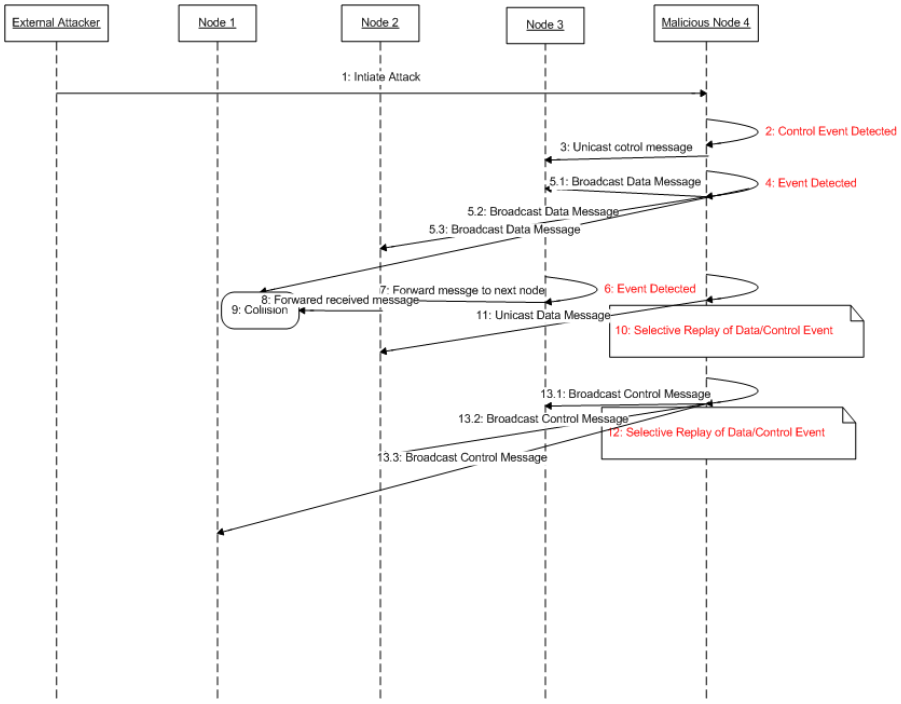

Figure 6 Sequence diagram for intelligent jamming attack.

4 ECN Attack for Hybrid MAC

4.1 Working Model

In case of a hybrid MAC mechanism such as Z-MAC (Zebra-MAC), an ECN message is used to notify all nodes in the network about a collision. The nodes will get the understanding of the contention by using ECN messages and they will act accordingly using this information. Figure 4 shows the normal processing along with the ECN attack. Figure 7(a) shows the three different paths from the intermediate node that may lead to contention at the intermediate node. The intermediate node experiences the contention and transmits the ECN message to all nodes in the network as shown in Figure 7(b). Figure 7(c) shows the ECN attack in which the malicious node, which has full knowledge of the MAC layer protocol used, will generate the ECN message and try to confuse the nodes, which disturbs the normal communication of the nodes and also incurs increased consumption of energy.

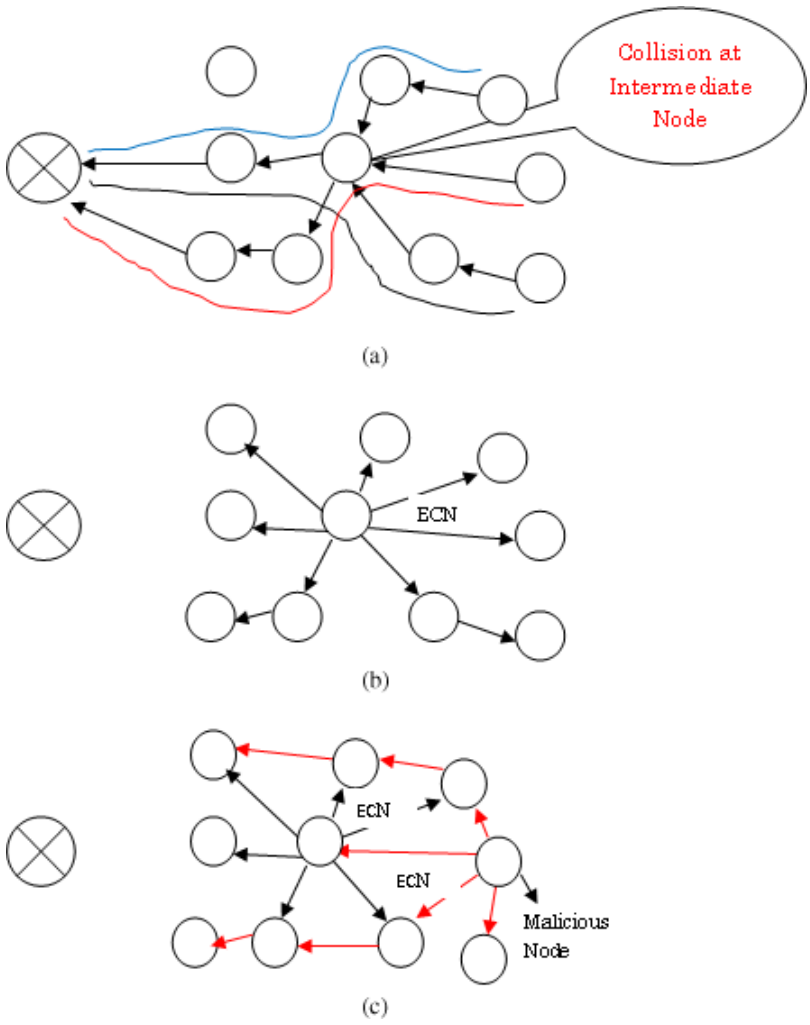

Figure 7 (a) Collision at intermediate node (b) Intermediate node sends an ECN message to all nodes for collision information (c) Attack in which malicious node will unnecessarily transmit the ECN message.

4.2 Behavioural Modelling of the ECN Attack

Figure 8 explains the flow of events in case of ECN attack. The details of each event are as follows,

- Node 4 detects the event and transmits the message towards the sink node via node 4->node 3->node 2-> node 1 to the sink node.

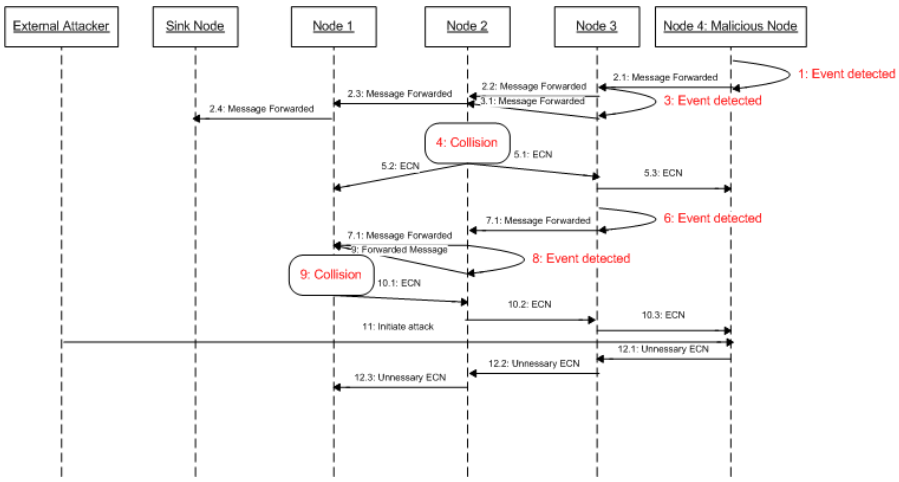

Figure 8 Sequence diagram for ECN attack.

During this transmission, node 3 will detect some event and tries to transmit towards the sink node and experiences the collision at the intermediate node 2. Node 2 measures the level of contention and transmits the ECN message to all one-hop and two-hop neighbours in the network.

- The same situation can be observed when node 3 and node 2 sense the event and experience the collision at node 1 after some time. Node 1 transmits the ECN message to the nodes in the network.
- The external attacker compromises the malicious node 4 by initiating an ECN attack. Once the attack is initiated the malicious node transmits the unnecessary ECN messages in the network and confuses the normal communication.

5 Conclusion

The applications of WSN are growing rapidly and these new applications have very stringent requirements concerning energy efficiency and security. In WSN, security is important at all layers because all layers are susceptible to security attacks. These security attacks directly affect the energy consumption and due to the large amount of energy consumed at the MAC layer, it is particularly vulnerable to many different security attacks. To protect the

MAC layer from attackers, it is necessary to understand the behaviour of the attacks so that secure MAC mechanisms can be developed. By better understanding the behaviour of the attacks, there is a better chance of finding solid solutions.

The UML based behavioural modelling of MAC security attacks gives this understanding of the behaviour of the attacks and the interaction of the system in presence of these attacks. This behavioural analysis is useful to develop efficient and secure solutions for the MAC layer.

In this paper, we also proposed the ECN attack that can be used in hybrid MAC mechanisms and we also give its behavioural modelling using UML. The attack drains the energy by introducing false ECN messages.

The future work will exploit UML modelling of MAC layer attacks using activity diagrams, implement security attacks on hybrid MAC mechanism and conduct performance evaluation on hybrid MAC algorithms in presence of attacks.

References

[1] Xiangqian Chen, Kia Makki, Kang Yen, and NikiPissinou. Sensor network security: A survey. *IEEE Communications Surveys & Tutorials*, 11(2): 52–73, Second Quarter 2009.

[2] Javier Lopez, Rodrigo Roman, and Cristina Alcaraz. *Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks*. Springer-Verlag Berlin Heidelberg, pp. 289–338, 2009.

[3] AbdelmalikBachir, MischaDohler, Thomas Watteyne, Kin K. Leung. MAC essentials for wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 12(2):222–248, Second Quarter 2010.

[4] Tom Peder. *UML Bible*. John Wiley & Sons, First Edition, 2003.

[5] Sunghyuck Hong and Sunho Lim. Analysis of attack models via unified modelling language in wireless sensor networks: A survey study. *WCNIS*, pp. 692–696, 25–27 Jan 2010.

[6] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmori, and Ramjee Prasad. Hybrid Mechanisms: Towards an Efficient Wireless Sensor Network Medium Access Control, WPMC, 3–6 October 2011, Brest, France.

[7] Injong Rhee, AjitWarrier, Mahesh Aia, Jeongki Min, and Mihail L. Sichitiu, ZMAC: A hybrid MAC for wireless sensor networks, *IEEE/ACM Transactions On Networking*, 16(3):511–524, June 2008.

[8] P. Reindl, K. Nygard, and Du Xiaojiang, Defending malicious collision attacks in wireless sensor networks, *EUC*, pp. 771–776, 11–13 Dec 2010.

[9] QingchunRen, Qilian Liang, Secure Media Access Control (MAC) in Wireless Sensor Network: Intrusion Detections and Countermeasures, PIMRC 2004, 3025–3029.

[10] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff. Effects of denial-of-sleep attacks on wireless sensor network MAC protocols. *IEEE Transaction on Vehicular Technology*, 58(1):367–380, January 2009.

[11] Yee Wei Law, Marimuthu Palaniswami, Lodewijk Van Hoesel, JeroenDoumen, Pieter Hartel, and Paul Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Transactions on Sensor Networks*, 5(1):6.1–6.38, Feb 2009.

[12] Yanli Yu, KeqiuLi, WanleiZhou, PingLi. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, March 2011.

[13] Michael Brownfield, Yatharth Gupta, and Nathaniel Davis IV. Wireless sensor network denial of sleep attack. In *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy*, West Point, NY, pp. 356–364.

Authors' Biography

Pranav M. Pawar graduated in Computer Engineering from Dr. BabasahebAmbedkar Technological University, Maharashtra, India, in 2005 and received Master in Computer Engineering from Pune Universiry, in 2007. From 2006 to 2007, was working as System Executive in POS-IPC, Pune, India. From Jan 2008, he is working as an Assistant Professor in Department of Information Technology, STES's Smt. KashibaiNavale College of Engineering, Pune. Currently he is working towards his Ph.D. in Wireless Communication from Aalborg University, Denmark. He published 17 papers at national and international level. He is IBM DB2 and IBM RAD certified professional. His research interests are Energy efficient MAC for WSN, QoS in WSN, wireless security, green technology, computer architecture, database management system and bioinformatics.

Rasmus Hjorth Nielsen is an assistant professor at Center for TeleInFrastruktur (CTIF) at Aalborg University (AAU), Denmark and is currently working as a senior researcher at CTIF-USA, Princeton, USA. He received his M.Sc. and Ph.D. in electrical engineering from Aalborg University in 2005 and 2009 respectively. He has been working on a number of EU- and industrial funded projects primarily within the field of next generation networks where his focus is currently security and performance optimization.

He has a strong background in operational research and optimization in general and has applied this as a consultant within planning of large-scale networks. His research interests include IoT, WSNs, virtualization and other topics related to next generation converged wired and wireless networks.

Neeli Rashmi Prasad, Ph.D., IEEE Senior Member, Head of Research and Coordinator of Themantic area Network without Borders, Center for TeleInfrastruktur (CTIF), Aalborg University, Aalborg, Denmark. Director of CTIF-USA, Princeton, USA and leading IoT Testbed at Easy Life Lab and Secure Cognitive radio network testbed at S-Cogito Lab. She received her Ph.D. from University of Rome "Tor Vergata", Rome, Italy, in the field of "adaptive security for wireless heterogeneous networks" in 2004 and M.Sc. (Ir.) degree in Electrical Engineering from Delft University of Technology, The Netherlands, in the field of "Indoor Wireless Communications using Slotted ISMA Protocols" in 1997. During her industrial and academic career for over 14 years, she has lead and coordinated several projects. At present, She is leading a industry-funded projects on Security and Monitoring (STRONG) and on reliable self organizing networks REASON, Project Coordinator of European Commission (EC) CIP-PSP LIFE 2.0 for 65+ and social interaction and Integrated Project (IP) ASPIRE on RFID and Middleware and EC Network of Excellence CRUISE on Wireless Sensor Networks. She is co-caretaker of real world internet (RWI) at Future Internet. She has lead EC Cluster for Mesh and Sensor Networks and Counsellor of IEEE Student Branch, Aalborg. She is Aalborg University project leader for EC funded IST IP e-SENSE on Wireless Sensor Networks and NI2S3 on Homeland and Airport security and ISISEMD on telehealth care. She is also part of the EC SMART Cities workgroup portfolio. She joined Libertel (now Vodafone NL), Maastricht, The Netherlands as a Radio Engineer in 1997. From November 1998 till May 2001, she worked as Systems Architect for Wireless LANs in Wireless Communications and Networking Division of Lucent Technologies, Nieuwegein, The Netherlands. From June 2001 to July 2003, she was with T-Mobile Netherlands, The Hague, The Netherlands as Senior Architect for Core Network Group. Subsequently, from July 2003 to April 2004, she was Senior Research Manager at PCOM:I3, Aalborg,

Denmark. Her publications range from top journals, international conferences and chapters in books. She has also co-edited and co-authored two books titled "WLAN Systems and Wireless IP for Next Generation Communications" and "Wireless LANs and Wireless IP Security, Mobility, QoS and Mobile Network Integration", published by Artech House, 2001 and 2005. Her research interests lie in the area of Security, Privacy and Trust, Management or Wireless and wired networks and Energy-efficient Routing.