Activity Modelling and Comparative Evaluation of WSN MAC Security Attacks

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

Activity Modelling and Comparative Evaluation of WSN MAC Security Attacks

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

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

Received ??; Accepted: ??

Abstract

Applications of wireless sensor networks (WSNs) are growing tremendously in the domains of habitat, tele-health, industry monitoring, vehicular networks, home automation and agriculture. This trend is a strong motivation for malicious users to increase their focus on WSNs and to develop and initiate security attacks that disturb the normal functioning of the network in a severe manner. Such attacks affect the performance of the network by increasing the energy consumption, by reducing throughput and by inducing long delays. Of all existing WSN attacks, MAC layer attacks are considered the most harmful as they directly affect the available resources and thus the nodes' energy consumption.

The first endeavour of this paper is to model the activities of MAC layer security attacks to understand the flow of activities taking place when mounting the attack and when actually executing it. The second aim of the paper is to simulate these attacks on hybrid MAC mechanisms, which shows the performance degradation of a WSN under the considered attacks. The modelling and implementation of the security attacks give an actual view of the network which can be useful in further investigating secure mechanisms to reduce the

Journal of Cyber Security and Mobility, Vol. 1, 1–20.

degradation of the performance in WSNs due to an attack. Lastly, the paper proposes some solutions to reduce the effects of an attack.

Keywords: wireless sensor networks (WSNs), media access control (MAC), activity modelling, security attacks.

1 Introduction

A WSN consists of small sensor nodes, each one equipped with limited battery, a microprocessor, a small amount of memory and a transducer. WSNs are versatile networks with a very wide domain of applications and their resource-constrained nature is an important research challenge. Like all other networks, WSN resources are mainly affected by the MAC layer and MAC layer protocols play an important role in resource utilisation, network delays, scalability and energy consumption [1].

Due to the rise of many mission critical WSN applications, another great challenge is security. The range and number of security attacks in WSNs have increased significantly over the last decade [2] and it is therefore necessary to design WSNs and related protocols also considering constraints with respect to security. Attacks can happen at all layer of a WSN but are more harmful when they are in the form of resource consumption attacks. Resource consumption attacks mainly take place at the MAC layer because this is the layer that controls the access to the resources in the network.

This paper focuses on denial of service MAC layer attacks in WSNs. Denial of service attacks in WSNs are primarily affecting the sleep mode of WSN nodes, which is often referred to as denial of sleep. During sleep mode, the nodes save energy by keeping the radio off and denial of sleep attacks prevent nodes from going into this mode, which increases the energy consumption and also reduces the total network lifetime [3, 4].

The objectives of this paper are to analyse the activities taking place in order to carry out the attack, to investigate how the attack can be implemented and to propose a solution that can reduce the effects of the attacks. The attacks are modelled using activity modelling, which is an efficient tool to understand the flow of activities during the implementation of the tasks. The attacks are implemented using the tool Network Simulator 2 (NS-2) considering hybrid MAC mechanisms [5] and the results show the actual performance degradation due to the attacks. The results are useful for proposing secure hybrid WSN MAC mechanisms and the paper proposes a novel solution that reduces the effect of a specific attack.

The remainder of this paper is organised as follows: Section 2 gives an overview of MAC layer denial of service/sleep attacks. Section 3 presents the activity modelling of security attacks. Section 4 discusses the simulation of security attacks and the results obtained and Section 5 explains the proposed solutions to reduce the effect of the attacks. Finally, Section 6 concludes the paper with future work.

2 MAC Layer Security Attacks

2.1 Collision Attack

The malicious collision attack [6, 7] can be easily launched by a compromised sensor node, which does not follow the MAC protocol rules and thereby causes collisions with neighbouring nodes' transmissions by sending short noise packets. This can cause a lot of disruptions to the network operation and will lead to retransmissions and wasted energy. The attack does not consume much energy of the attacker and it is difficult to detect because of the broadcast nature of the wireless environment.

2.2 Unintelligent Replay Attack

In case of the unintelligent replay attack [3], 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 energy at each relaying node on the path to the destination. The replaying of events has adverse effect on the network lifetime and overall performance of a WSN.

2.3 Unauthenticated Broadcast Attack

In an unauthenticated broadcast attack [3], the attacker has full knowledge of the MAC protocol but does not have the capability to penetrate the network. Here, the attacker broadcasts unauthenticated traffic into the network by following all MAC rules and this disrupts the normal sleep and listen cycle of the node and places most of the nodes in listen mode for an extended amount of time, which leads to increased energy consumption and reduction in network

lifetime. Such attacks cause severe harm on MAC protocols by producing short control or data messages and have short adaptive timeout period.

2.4 Full Domination Attack

Here, the attacker has full knowledge of the MAC layer protocol and has the 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. This attack is carried out using one or more compromised nodes in the network and all MAC layer protocols are vulnerable to this kind of attack [3].

2.5 Exhaustion Attack

The attacker who commences an exhaustion attack [3] 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 energy of the node. This attack is affecting the node lifetime and can partition the network, which lead to reduced network lifetime.

2.6 Intelligent Jamming Attack

The intelligent jamming attack is one of the most severe attacks and in this attack the 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 and data traffic and unlike the unauthenticated replay attack it selectively replays the data or control packets [3, 8].

3 Activity Modelling of MAC Security Attacks

3.1 Activity Modelling

Activity diagrams are often used to give a functional view of a system as it describes logical processes, or functions, where each process describes a sequence of tasks and the decisions that govern when and how they are performed. UML [9–11] is a tool that provides functional modelling in the

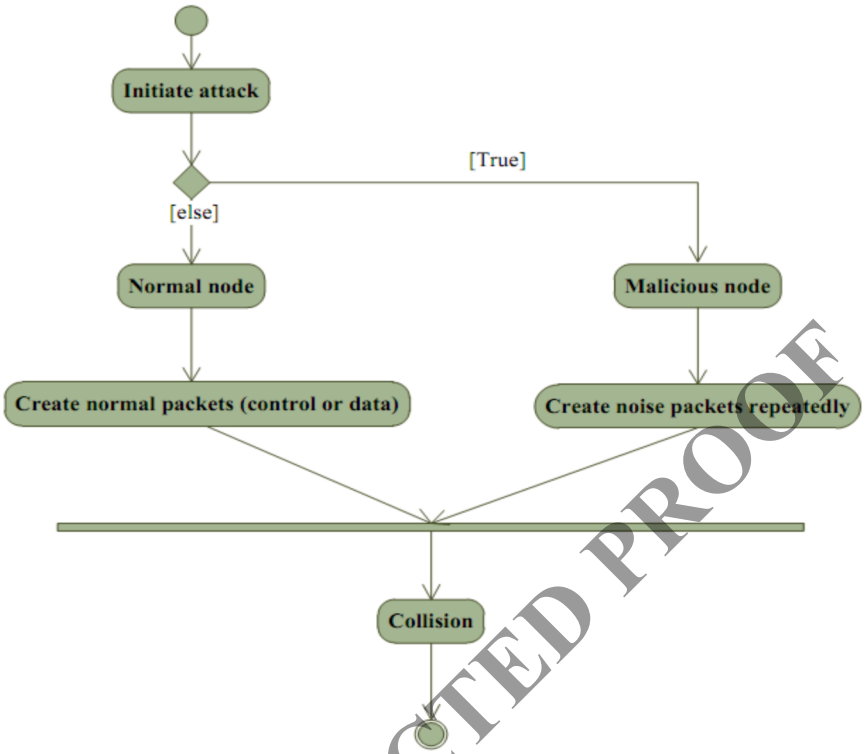


Figure 1 Activity modelling of collision attack.

form of an activity diagram, which is designed to support the description of behaviours that depend upon the results of internal processes, as opposed to external events as in interaction diagrams. The flow in an activity diagram is driven by the completion of an action. Activity diagrams are useful tools to understand the basic flow of security attacks and will be utilised in the following to do so.

3.2 Activity Modelling of Security Attacks

For all of the presented attacks, the external attacker will have to initiate an attack by utilising an exploit on a vulnerable normal node to turn it into a malicious node. If the attacker succeeds in initiating the attack the normal node becomes malicious and otherwise it continues to operate as a normal node.

3.2.1 Collision Attack

Figure 1 shows the activity diagram for the collision attack and the different activities are as follows:

- The malicious node randomly creates noise packets and transmits them into the network.
- A normal node starts a transmission to the sink either by direct communication or through relays using multi-hop communication.
- A collision happens between the control or data packet from the normal node and the noise packet from the malicious node. Repeatedly collisions will reduce the performance of the network.

3.2.2 Unintelligent Replay Attack

The sequence of activities in case of an unintelligent replay attack is shown in Figure 2 and are as follows:

- The normal node has data to send and checks if the channel is available and, if it is, the node starts the transmission.
- The malicious node records the transmission as if in normal node mode, which it keeps replaying unintelligently, i.e. without making differentiation between data and control packets; it will replay any transmission the normal node would have generated.
- The malicious node checks the remaining energy on each replay and once the energy is exhausted, the attack will be terminated and the external attacker will try to initiate the attack on another node.

3.2.3 Unauthenticated Broadcast Attack

Figure 3 shows the activity modelling of the unauthenticated broadcast attack. The sequence of activities performed by the normal and malicious node is as follows:

- The normal node does communication as in the previous attack.
- The malicious node uses similar transmissions, but broadcasts the packet to all nodes in the network and, further, tries to authenticate itself, which fails.
- If the broadcast takes place during transmission of a normal node a collision will take place. These collisions and the failed attempt to authenticate lead to performance degradation and thereby excessive energy consumption.

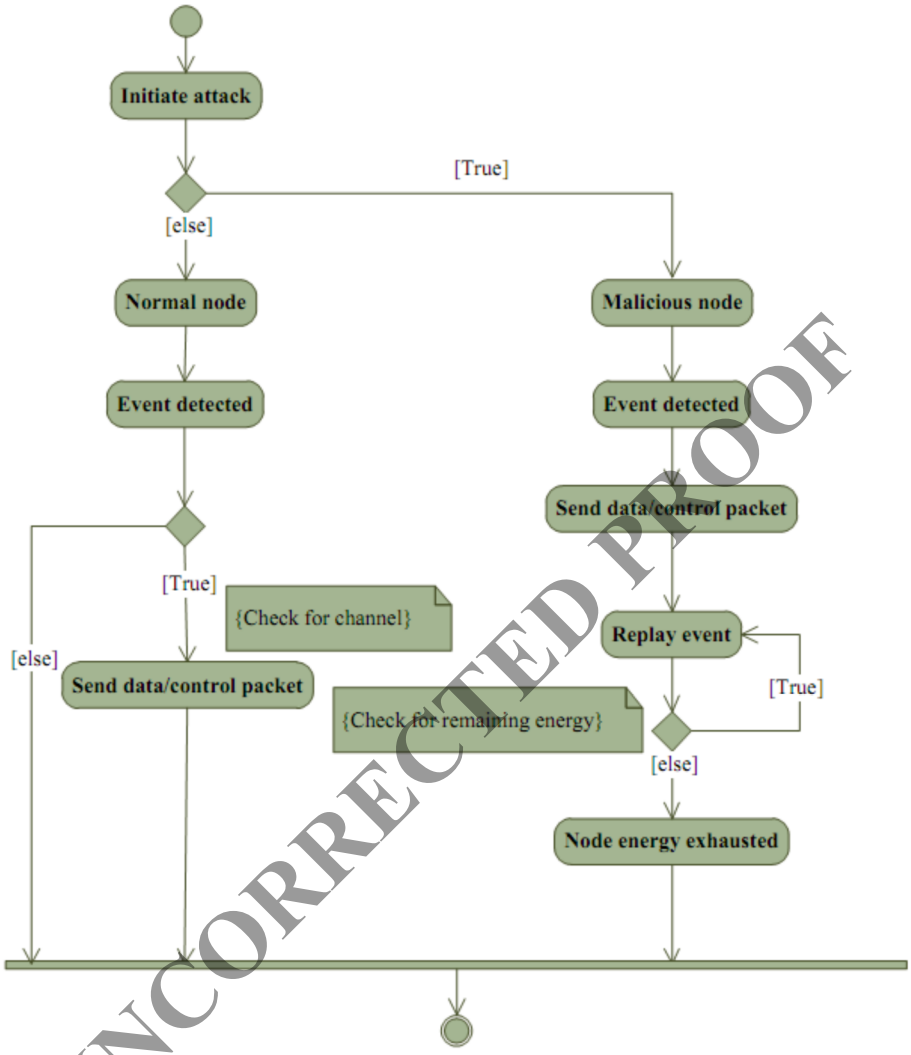


Figure 2 Activity modelling of unintelligent replay attack.

3.2.4 Full Domination Attack

The modelling of the sequence of activities for the full domination attack can be seen from Figure 4 and activities are as follows:

- The normal node broadcasts a packet into network, if the channel is available.

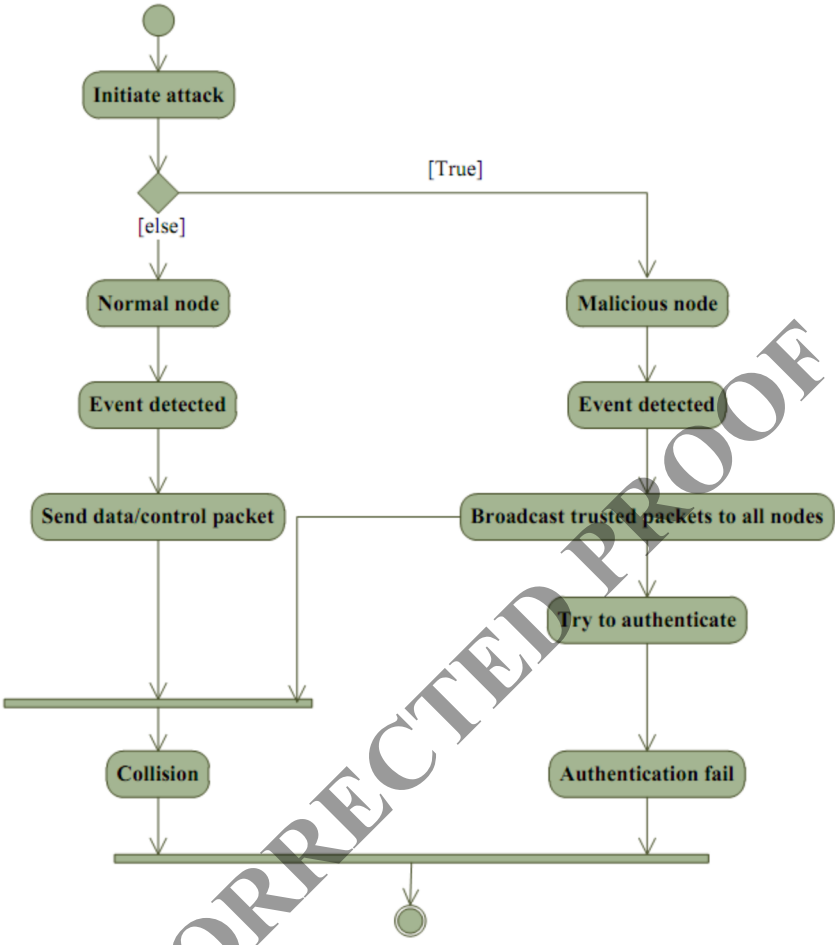


Figure 3 Activity modelling of unauthorised broadcast attack.

- The malicious node does the same and tries for authentication. As the attacker has full network knowledge, the authentication is successful and the malicious packet is transmitted while the malicious node tries to introduce collisions during normal traffic.
- The malicious node can also replay the communications unintelligently and broadcast it until the node's energy is exhausted. The full domination attack reduces the efficiency of the network by introducing authenticated broadcast and by replaying transmissions.

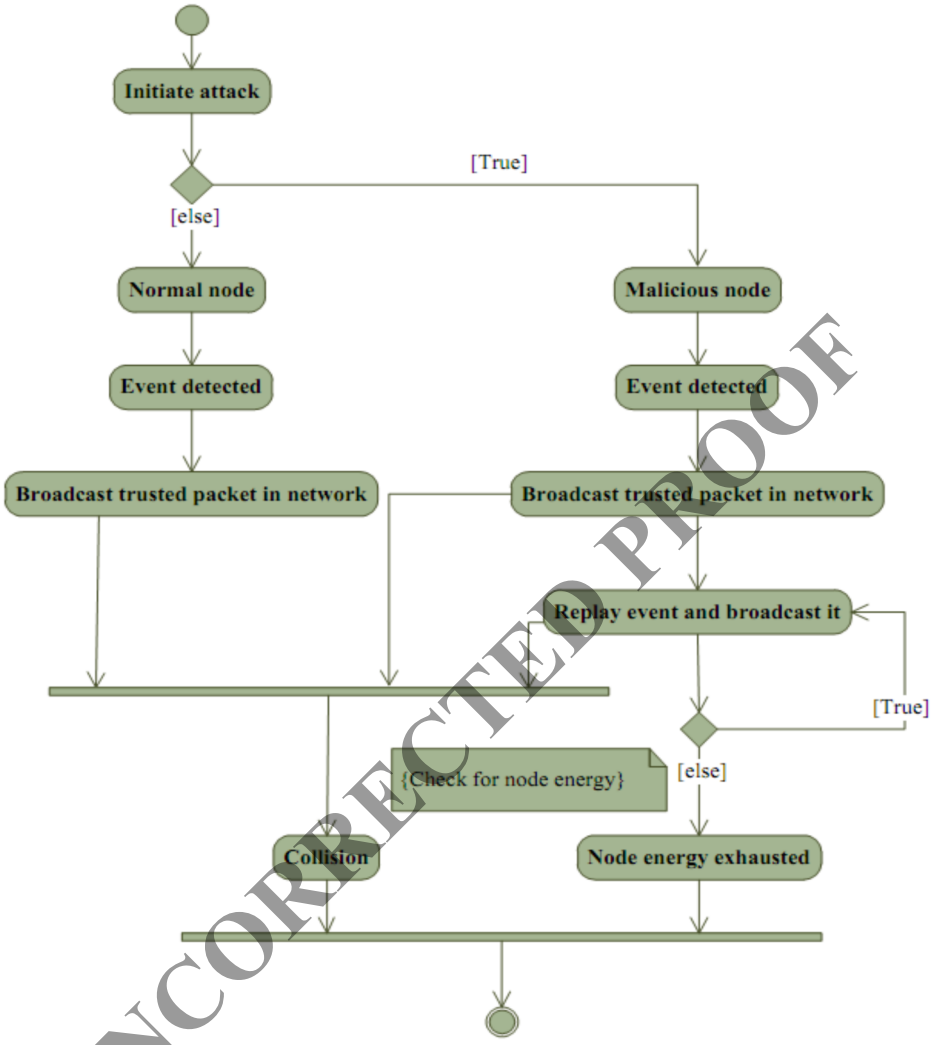


Figure 4 Activity modelling of full domination attack.

3.2.5 Exhaustion Attack

Figure 5 explains the sequence of activities during an exhaustion attack and the sequence of activities can be explained as follows:

- The normal node can send RTS, receive CTS from destination and send data towards the destination node.

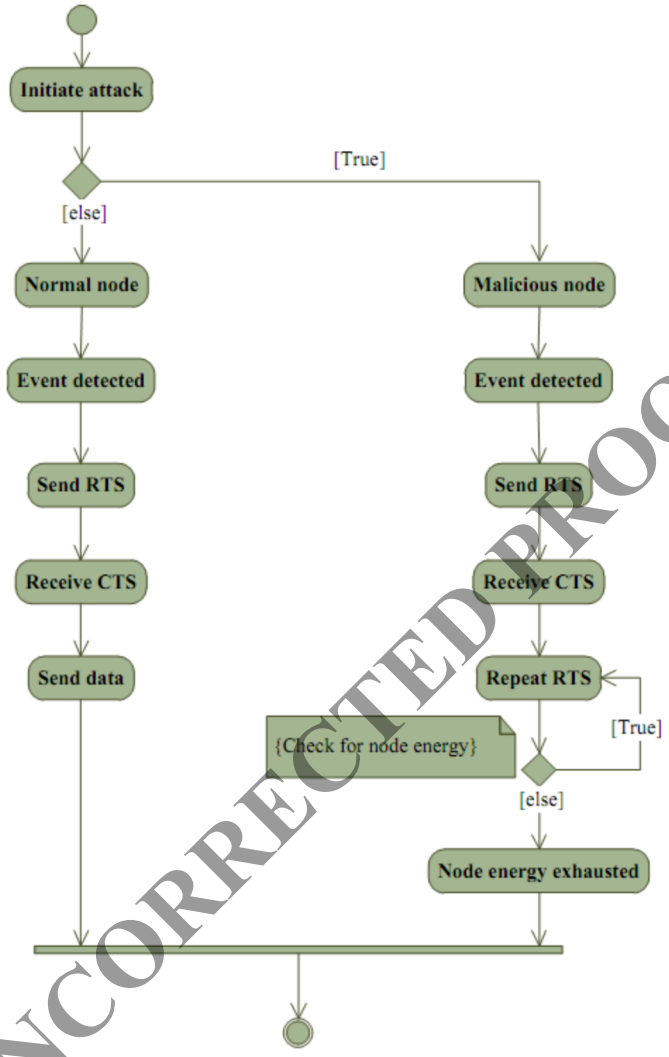


Figure 5 Activity modelling of exhaustion attack.

- In case of the malicious node, it sends RTS and waits for CTS from the destination node. If it receives the CTS, it will send the RTS repeatedly towards the destination node until its energy is exhausted.

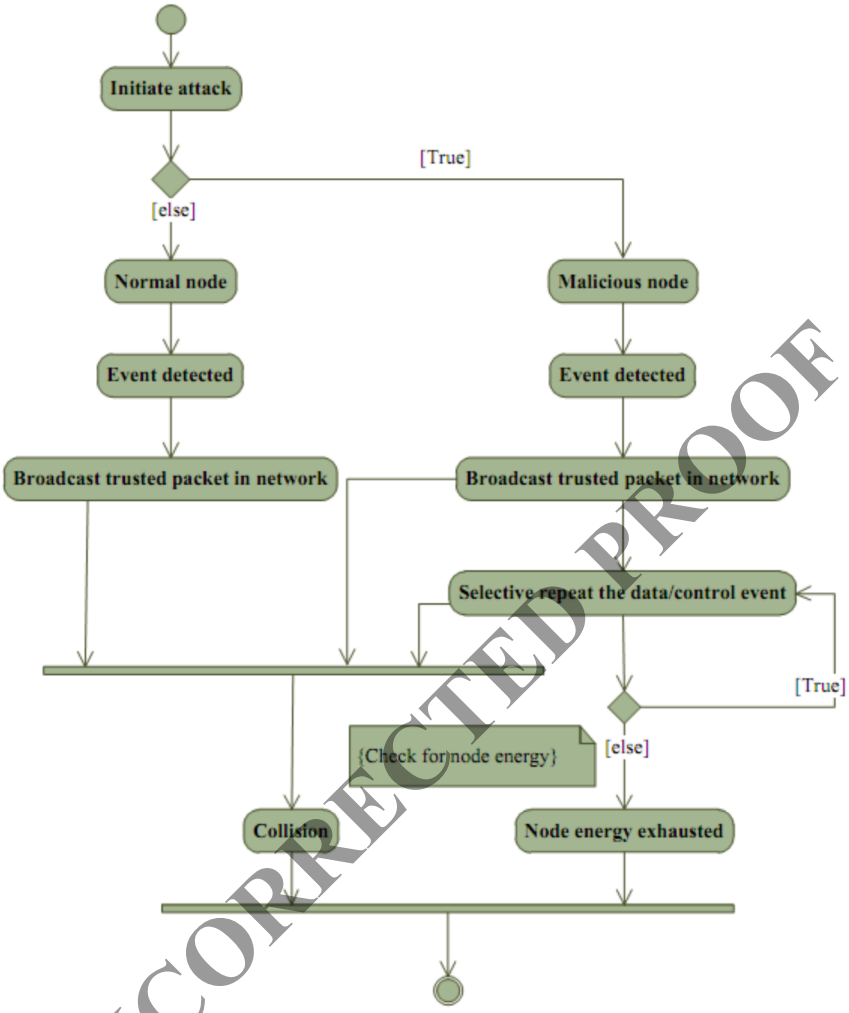


Figure 6 Activity modelling of intelligent jamming attack.

3.2.6 Intelligent Jamming Attack

Figure 6 shows the sequence of activities that happen during an intelligent jamming attack and the activities are as follows:

- The normal node has data to send and broadcasts it if the channel is available.

- The malicious node does the same, authenticates to the node and broadcasts the packet in the way as for the full domination attack.
- The most important feature of the intelligent jamming attack is its intelligent behaviour. It can differentiate between data and control packets, and will selectively replay the event until the node energy is exhausted.
- The replaying of event and broadcast of authenticated packet lead to collisions during normal transmissions.

4 Simulation of Security Attacks on Hybrid WSN MAC

4.1 Simulation Details

All simulations are carried out using the discrete event simulator NS-2 and the simulation parameters are shown in Table 1. The idle power, receiving power, transmission power and sleep power are considered according to the RFM TR 3000 transceiver. The simulations are performed using the hybrid MAC mechanism Zebra-MAC (ZMAC) [11] and the simulated scenarios are:

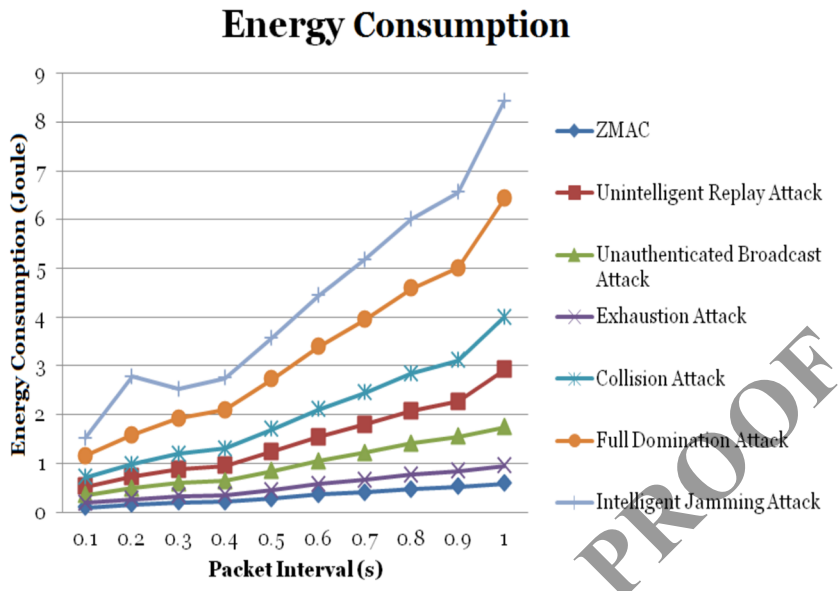
- ZMAC without any attacks.
- ZMAC under unintelligent replay attack.
- ZMAC under unintelligent broadcast attack.
- ZMAC under exhaustion attack.
- ZMAC under collision attack.
- ZMAC under full domination attack.
- ZMAC under intelligent jamming attack.

The simulations are carried out under the assumption that the attacker can initiate the attack from multiple nodes. The initial simulation is done using four malicious nodes, but the impact of varying malicious nodes (2–32) is also investigated.

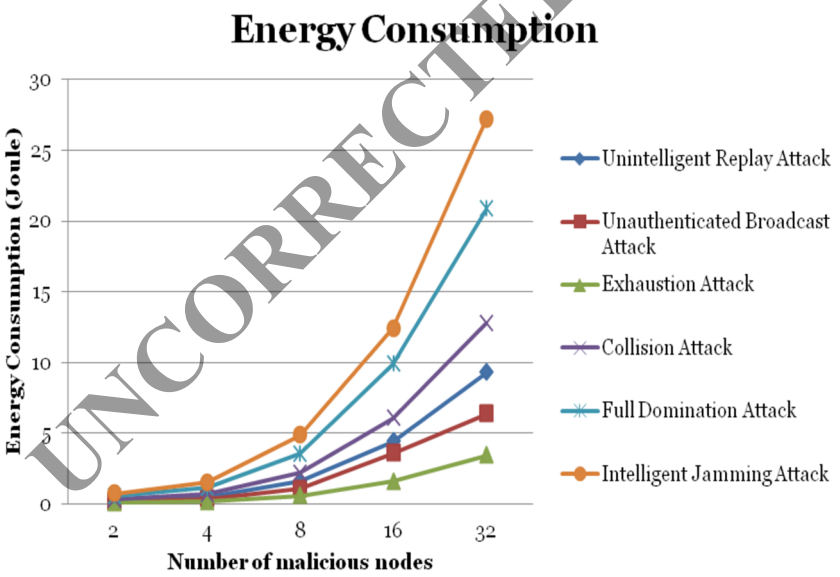
4.2 Results and Discussion

Figures 7–9.3 show the performance, i.e. energy consumption, throughput and delay of ZMAC, a hybrid MAC mechanism, under normal conditions and under attacks. The figures show that the performance of the WSN degrades with the attacks and the reasons for the performance degradations under the individual attacks are as follows:

- Unauthenticated Broadcast Attack: The performance degradation due to this attack is less compared to the other attacks because this attack utilises more energy and requires extra time for authentication of the

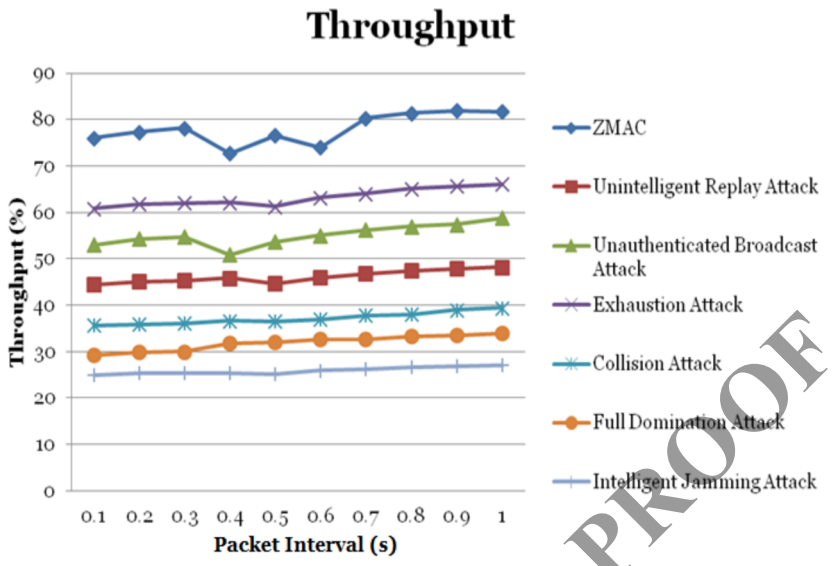


(a) Energy consumption vs. packet interval

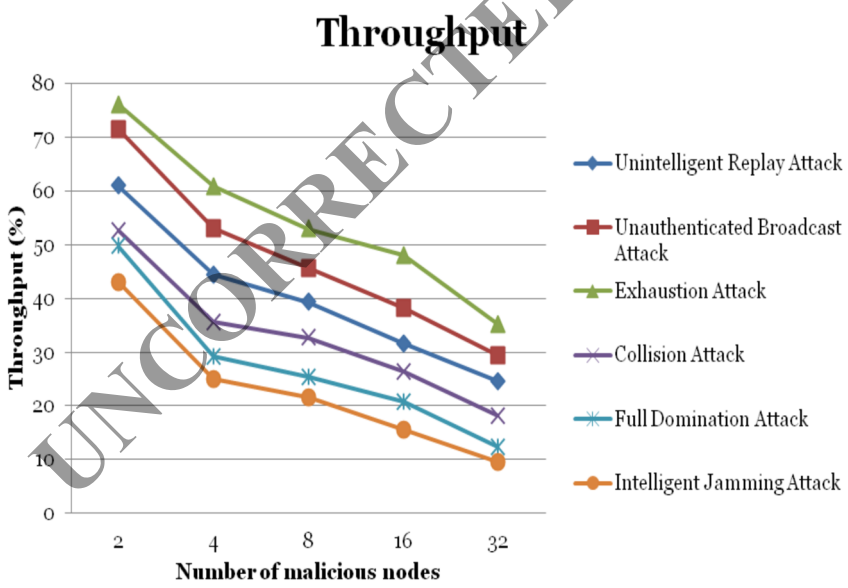


(b) Energy consumption vs. number of malicious nodes

Figure 7 (a) Energy consumption vs. packet interval. (b) Energy consumption vs. number of malicious nodes.

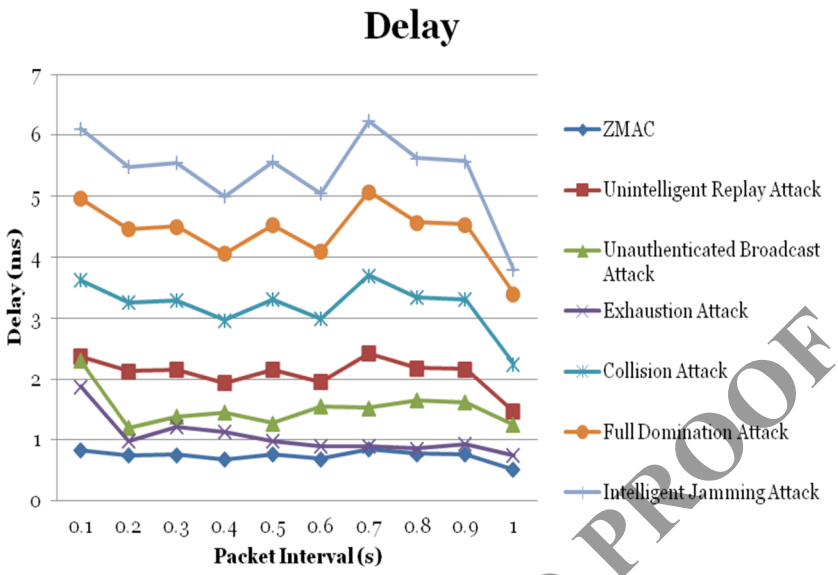


(a) Throughput vs. packet interval

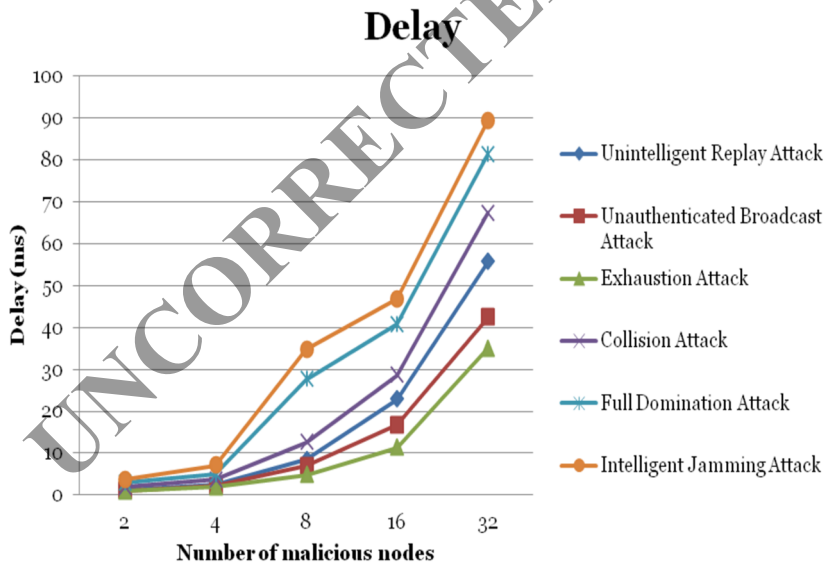


(b) Throughput vs. number of malicious nodes

Figure 8 (a) Throughput vs. packet interval. (b) Throughput vs. number of malicious nodes.



(a) Delay vs. packet interval



(b) Delay vs. number of malicious nodes

Figure 9 (a) Delay vs. packet interval. (b) Delay vs. number of malicious nodes.

Table 1 Simulation and node parameters.

Parameter Name	**Setting Used**
Wireless Physical	
Network Interface Type	Wireless Physical
Radio Propagation Model	Two-Ray Ground
Antenna Type	Omni-directional antenna
Channel Type	Wireless Channel
Link Layer	
Interface Queue	Priority Queue
Buffer Size of IFq	50
MAC	Z-MAC
Routing Protocol	Ad hoc Routing
Energy Model	
Initial Energy (initialEnergy_)	100 J
Idle Power (idlePower_)	14.4 mW
Receiving Power (rxPower_)	14.4 mW
Transmission Power (txPower_)	36.0 mW
Node Placement	
Number of Nodes	100
Node Placement	Random

broadcast packets coming from the malicious nodes. The attack results in degradation of the total throughput of the network due to an increased number of collisions caused by the unauthenticated packets and the following retransmission of packets from trusted nodes.

- Unintelligent Replay Attack: The performance degradation due to this attack is more severe than for the unauthenticated broadcast attack because this attack increases the energy consumption by replaying data or control packets and thereby wastes energy. A significant increase in delay can be observed because the node checks for energy at each replay and also requires additional time to carry out the replay. This unnecessary replay keeps the channel busy, which may introduce collisions and prevent transmission of other packets, which results in degradation of the total throughput of the network. The attack has more severe performance degradation than the unintelligent replay attack because it can take place in any situations, i.e. (i) no protocol knowledge, no ability to penetrate, (ii) full protocol knowledge, no ability to penetrate, and (iii) full protocol knowledge, network penetrated.
- Exhaustion Attack: The most adverse effect of this attack is that it totally blocks the transmission towards one particular node and blocks this node until its energy is depleted or the network becomes partitioned.

- Collision Attack: The noise packets introduced by this attack result in significant performance degradation due to the increased number of collisions in the network. The collisions result in performance degradation by (i) blocking the channel, (ii) increasing the retransmission of packets, (iii) introducing delays, and (iv) reducing the chances of packets to reach their destination. The effect of collisions is adverse as the traffic load increases.
- Full Domination Attack: This attack is a combination of the previously two attacks and therefore has more adverse effects. The results shows that energy, throughput and delay degradation is much increased compared to the previous attacks as this attack increases the delay and energy by repeatedly broadcasting packets which makes the channel constantly busy, so it will not be available other nodes to transmit and it also reduces the throughput by not giving the chance to new packets to be transmitted through the network. As for the exhaustion attack, it also partition the network but much faster.
- Intelligent Jamming Attack: This is the most disastrous of the considered attacks because it works intelligently by selectively retransmitting data and control packets. It requires in-depth knowledge of the protocols used in the network. The results show that the performance degradation of this attack is slightly more severe than the full domination attack as this attack cannot intelligently retransmit.

5 Proposed Solutions

The implementation shows the adverse effect on the network of the listed WSN MAC layer attacks. The attacks degrade the performance of the WSN with 50% or more and to reduce these effects some possible solutions are

- Cluster-based MAC protocol: Cluster-based MAC protocols improve the scalability of the network by stabilising the network topology at the level of sensors and thus lower the topology maintenance overhead. The clustering can also reduce the number of required slots by increasing the reuse of slots that, in turn, can reduce the amount of delay in communication. One important advantage offered by cluster-based protocols is their inherent security, as an attack on a cluster based MAC protocols will be bound to that particular cluster and not affect the whole network. This automatically reduces the overall impact of the attack on the total performance of the WSN.

- Secure slot assignment: Secure slot assignment assumes that some slots are secure and are given only to nodes that are transmitting sensitive information. Nodes with secure slots assigned can start communication with another node by checking the identity of the node to determine if it is secure to communicate or not. This will help to reduce the influence of MAC security attacks in terms of reducing energy consumption, delay and increasing throughput.

6 Conclusion

The activity modelling of WSNs MAC layer security attacks gives a detailed view of activities executed during mounting of the attacks, which is essential knowledge for proposing more efficient security mechanisms that can withstand the attacks. The paper also provides simulation results of security attacks on a hybrid MAC mechanism and the results show the trend of network degradation due to the security attacks under varying traffic and number of malicious nodes. Intelligent jamming attacks pose the greatest threat to a WSN because of its intelligent nature, i.e. the attacker has full knowledge of the protocols used, it can easily differentiate between control and data packets and it can penetrate the network. The simulation results in general give a strong motivation and modelling framework for further investigating efficient and secure MAC protocols for WSN.

References

[1] Bachir, A., Dohler, M., Watteyne, T., and Leung, K.K., MAC essentials for wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 12(2):222–248, 2010.

[2] Chen, X., Makki, K., Yen, K., and Pissinou, N. Sensor network security: A survey. *IEEE Communications Surveys & Tutorials*, 11(2):52–73, 2009.

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

[4] Brownfield, M., Gupta, Y., and Davis IV, N. Wireless sensor network denial of sleep attack. In *Proceedings of IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, NY, 15-17 June, pp. 356–364, 2005.

[5] Pawar, P.M., Nielsen, R.H., Prasad, N.R., Ohmori, S., and Prasad, R. Hybrid mechanisms: Towards an efficient wireless sensor network medium access control. In *Proceedings of WPMC*, Brest, France, 3–6 October, pp. 492–496, 2011.

[6] Reindl, P., Nygard, K., and Xiaojiang, Du. Defending malicious collision attacks in wireless sensor networks. In *Proceedings EUC*, Hong Kong, China, 11–13 December, pp. 771–776, 2010.

[7] Ren, Q. and Liang, Q. Secure Media Access Control (MAC) in wireless sensor network: Intrusion detections and countermeasures. In *Proceedings PIMRC*, Berlin, Germany, 5–8 September, pp. 3025–3029, 2004.

[8] Law, Y.W., Palaniswami, M., Van Hoesel, L., Doumen, J., Hartel, P., and Havinga, P. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. *ACM Transactions on Sensor Networks*, 5(1):6.1–6.38, February 2009.

[9] Peder, T. *UML Bible*, First Edition. John Wiley & Sons, 2003.

[10] Pawar, P.M., Nielsen, R.H., Prasad, N.R., Ohmori, S., and Prasad, R. Behavioural modelling of WSN MAC layer security attacks: A sequential UML approach. *Journal of Cyber Security and Mobility*, 1(1):65–82, January 2012.

[11] Hong, S. and Lim, S. Analysis of attack models via unified modelling language in wireless sensor networks: A survey study. In *Proceedings WCNIS*, Beijing, China, 25–27 January, pp. 692–696, 2010.

[12] Rhee, I., Warrier, A., Aia, M., Min, J., and Sichitiu, M.L. ZMAC: A hybrid MAC for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 16(3):511–524, June 2008.

Biographies

Pranav M. Pawar graduated in Computer Engineering from Dr. Babasaheb Ambedkar Technological University, Maharashtra, India, in 2005 and received a Master in Computer Engineering from Pune Universiry, in 2007. From 2006 to 2007, was working as System Executive in POS-IPC, Pune, India. From January 2008, he has been 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 an 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,

Shingo Ohmori ■■Please, supply missing biography■■

Ramjee Prasad ■■Please, supply missing biography■■