An Ontology for Attacks in Wireless Sensor Networks

Wassim Znaidi, Marine Minier, Jean-Philippe Babau

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

An Ontology for Attacks in Wireless Sensor Networks

Wassim Znaidi, Marine Minier and Jean-Philippe Babau

N° 6704

Octobre 2008

Thème COM

ISSN 0249-6399 ISRN INRIA/RR--6704--FR+ENG

INRIA
RHÔNE-ALPES

An Ontology for Attacks in Wireless Sensor Networks

Wassim Znaidi, Marine Minier and Jean-Philippe Babau

Thème COM — Systèmes communicants
Projet Amazones

Rapport de recherche n° 6704 — Octobre 2008 — 13 pages

Abstract: Wireless sensor networks (WSNs) have many potential applications. In many scenarios WSNs are of interest to adversaries and they become susceptible to some types of attacks since they are deployed in open environments and have limited resources. Many attacks are known against WSNs. Protections exist against some of them but for the others IDS (Intrusion Detection Mechanism) systems are required. In this report, we present a new WSN attacks ontology that enable us to identify the intention of the attacker, his capabilities to achieve the attacks, the target and the end result. This ontology is a high level abstraction that does not depend on the IDS system used. We also survey known vulnerabilities and attacks in WSNs and present some defenses.

Key-words: attacks, wireless sensor networks, ontology

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier (France)
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Une ontologie des attaques dans les réseaux de capteurs sans fil

Résumé : Les réseaux de capteurs sans fil ont beaucoup d'applications potentielles. Dans beaucoup de scénarios, ces réseaux sont sujets à de nombreuses attaques en raison du déploiement en environnement ouvert et de leurs ressources limitées. Des mécanismes de protection existent contre quelques unes d'entre elles mais il est souvent nécessaire d'ajouter à ces systèmes des mécanismes de détection d'intrusion. Dans ce rapport, nous présentons une nouvelle ontologie d'attaques dans ces réseaux afin d'identifier l'intention de l'attaquant, ses capacités à réussir les attaques, la cible et le résultat final. Cette ontologie est une abstraction de haut niveau qui ne dépend pas du système d'intrusion utilisé. Nous décrivons également ici les vulnérabilités connues dans les réseaux de capteurs sans fil et nous présentons également un certain nombre de contre-mesures.

Mots-clés : attaques, réseaux de capteurs sans fils, ontologie

1 Introduction

Advances in wireless communications have enabled the development of low-cost and low-power wireless sensor networks (WSNs). The characteristics of such WSNs are namely minimal energy, weak computational capabilities, wireless communication and an open-environment nature where sensors are deployed. Due to the intrinsic nature of those networks, WSNs are vulnerable to many attacks. Some of those attacks can be discarded by preventive mechanisms but IDS schemes are required to prevent the others. In this paper, we present a new ontology to categorize attacks in WSNs. This high level ontology does not depend on the IDS system used, it highlights the link between some actions done in the network and the possible attacks coming from those observed facts. Moreover, we outline the known attacks on WSNs and relative solutions.

The rest of this paper is organized as follows: in section 2 we define a new ontology attacks in order to better classify attacks on sensor networks. In section 3 we focus on attacks and vulnerabilities along with possible defenses and we show how we can apply the ontology to such attacks.

2 Attacks Ontology

Several attack classifications have been proposed in the literature. The main approaches used to describe and classify attacks are: taxonomies and ontologies. A taxonomy allows us to reason about attacks at a higher level than a simple list of vulnerabilities and so provides a system classification that helps designer to minimize attacks. A good taxonomy [1] must have the following characteristics: *accepted*, *unambiguous*, *comprehensible*, *determinist*, *mutually exclusive* and *exhaustive*. [19, 8, 14, 22] propose different taxonomies to classify attacks. Then ontologies were proposed to limit the inefficiency and the inexpressiveness of attack taxonomies. An ontology is a structured system of concepts which covers a specific field and presents the reality in a form of a model.

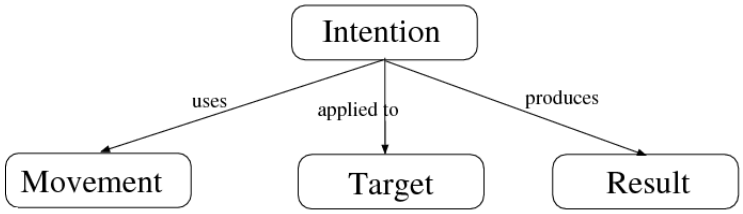
2.1 Ontology for Wireless Sensor Network

Here we present our ontology to classify WSN's attacks which was inspired from work in [6]. In their work, the authors define a new alerts ontology with abstraction of detectors which means they propose a new model of the detectors without consider any specific IDS (Intrusion Detection System). This abstraction is done using the theory of action in philosophy which roughly says that an action is composed of an intention, a movement and an object. So, we propose to implement these concept for WSN. Using this approach, our attack ontology (shown in Figure 1-a) is composed by four main classes, *intention*, *movement*, *target* and *result*. In our ontology, we do not take into account the nature of the attacker (if it was a raider, a hacker, a vandal, etc) because we assume that once the malicious node is introduced in the network, it is very difficult to define his nature and to distinguish it with a legitimate node.

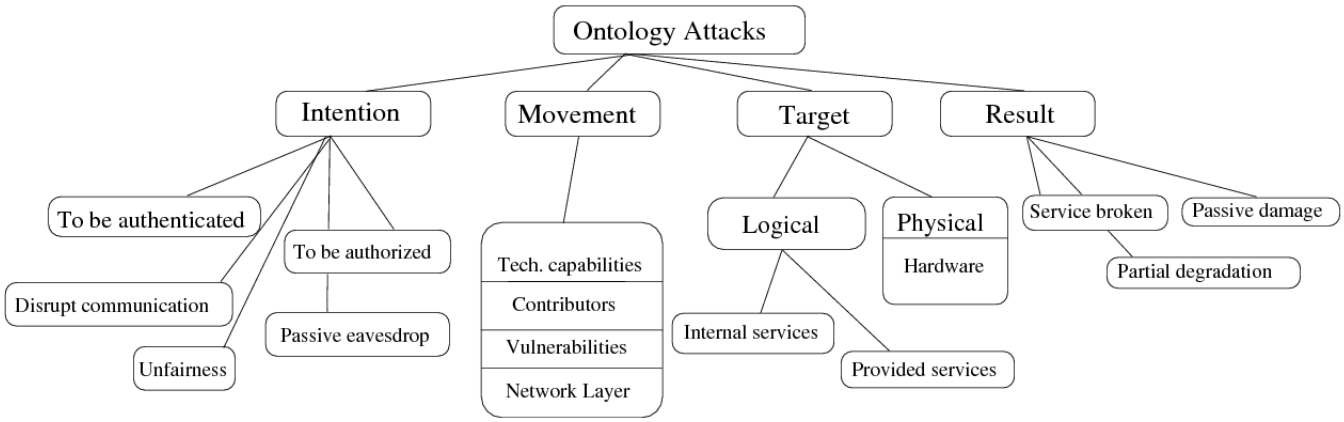
2.1.1 Intention

Each attack in the network has a plan of action. This plan can be composed by one or many steps which correspond to the achievement of a goal (the goal can also be viewed as the sum of multiple sub-goals). As we want to identify the intention of an attacker, we must first study his attack strategy. This plan can be organised in three phases: information gathering, exploits and contamination.The information gathering consists in determination of characteristics and weaknesses of the WSN as the topology discovery, location of the sink, traffic analysis, etc. Once information collected, the attacker try to find vulnerabilities that can be exploitable (exploits) as determination of the master/private key, alteration of data packets, etc, and finally once the attack is set up, the contamination phase presents the influence on the other parts of the network. Using this study, we now define five different intentions for an attack in a WSN :

- *Passive eavesdrop*, which consists in information gathering on specific or multiple targets.
- *Disrupt communication*, which consists in preventing data from reaching their destinations and destroying links between nodes.
- *Unfairness*, which ensures the exhausting of available resources like bandwidth, energy, battery, etc.
- *To be authenticated*, which means obtaining a right access to the network services.



(a) The ontology attacks.



(b) The ontology viewed as a taxonomy.

Figure 1: Ontology attack.

- *To be authorized*, which means having the ability to grant appropriate access to ressources, for example obtain keys to decrypt messages.

2.1.2 Movement

The movement describes the way the attacker reaches one/many intentions presented above. We identify four different categories that describe the movements in a wireless sensor networks:

- *Technical capabilities*, which means the extra technologies available with the malicious entity : for example an attacker may have a sophisticated wireless radio to receive and transmit over multiple channels. It may have also more efficiency hardware component, higher bandwidth links and better batteries. The attacker can also use a laptop to apply efficient tamper techniques to extract data from nodes.
- *Contributors*, which specify if the attack is realized by one or many adversaries. How do these attackers cooperate together to success the attack ? Are they autonomous or centrally controlled ? Is the attacker a sample sensor node or a sophisticated device ? A laptop for example ? All this characteristics differ from one attacker to another.
- *Vulnerabilities*, which are the weaknesses present in the network due for example to resources constraints or wicked design.Vulnerabilities can be *physical* - for example a tamper attack is very easy to launch as the nodes are deployed in open environment - or *logical* - designing and implementing vulnerabilities such as buffer overflows, bad configurations or resources exhaustions.
- *Layer*, here we precise which network layer the attack uses to success its intention. The network layers are physical, link, routing and application.

2.1.3 Target

In a WSN, all system resources and network services are targets for the attackers. Targets can be *physical*, for example destroy the sensor, damage the radio, remove the batteries, etc. Targets can be *logical*: *internal* or *provided* services. An attack against an internal service has the goal to damage an intern service of the sensor node, for example the power management, connection between layers, etc. However provided service concern services available in the network such as time synchronization, key management, clustering protocols, etc.

2.1.4 Result

An attack is considered successful if the global goal is achieved. But sometimes, the attack can be partially achieved and not completed. So we can define three categories to describe the result:

- If the attack was stopped by a preventative mechanism, we can say that we have a *passive damage*. So the service offered by the WSN is not damaged.
- If the service is absent in one part of the network (for example in one cluster region), here the attacker maybe has *partial degradation* of the WSN duty.
- the most serious problem is when the service is *broken* for the entire network.

Figure 1-b summarises our ontology presented as a taxonomy for simplification reasons.

3 Attacks on WSNs and defenses

In the following section, we describe some attacks of WSNs and possible defenses. Attacks described below are classified using network layers for only simplification reasons. We will also show how we can apply our ontology described in section 2 to classify those attacks examples.

3.1 Attacks on physical layer

3.1.1 Jamming

In a jamming attack, the adversary tries to transmit signals to the receiving antenna at the same frequency band or sub-band as the transmitter uses, thus causing radio interference. This attack is mostly used by a laptop, which holds higher energy, to disrupt continuously the network. It can also be done with a simple node causing a partial damage which can be also fatal to the WSN (for example random distributed jammed node). In [29] authors present different jamming strategies: *constant jamming* by emitting continuously a radio signal, *deceptive jamming* by injecting regular packets to the channel without any gap between packets, *random jamming* where the attacker alternates between sleeping and jamming to save power consumption and *reactive jamming* which will transmit only when it senses channel activity and will stay quiet when the channel is idle [17]. Many solutions have been proposed to defend against these jamming attacks. Typical defenses involve variations of spread-spectrum communication such as frequency-hopping spread spectrum (FHSS), that consists in sending data by switching rapidly a carrier sense among many frequency channels, or code spreading. The FHSS techniques are only used in military applications due to the complexity and to the cost, for example the MICA 2 mote is the only known sensor which switches efficiently between two frequency and every extra frequency will need extra processing. [29] proposes others solutions against jamming attacks. Nodes can also try to map out the jammed area by isolating the infected region. Such a protocol was presented in [28]. Another option is to use channel surfing method which is motivated by frequency hopping modulation. The difference with FHSS is that channel surfing does not involve a continual change of the carrier sense and it operates at the link layer. According to the ontology, the intention of the jamming attack is to disrupt communication. The movement is a sophisticated radio as technical capability, one/many node or a laptop as contributors, wireless communication and known channel as vulnerabilities and it uses the physical layer. The target will be the communication services and the result is partial/entire degradation of the services in the network.

3.1.2 Tampering

Another possible attack is tampering which involves physical access and capture of nodes. The adversary can gain full control of these motes and try to extract sensitive information such as secret key shared between

nodes. The tampering attacks can be classified into two classes: *invasive* attacks, which require access to the hardware components like chips and which need high-tech and expensive equipment used in semiconductor manufacturing, and *non-invasive* which are easiest than invasive and require less times. In [4], the authors had tried some of those attacks on Telos and Mica2 motes. We can mention attack via JTAC[1] such as testing access port (TAP) which can enable an adversary to take complete control over the sensor node. Other attacks consist on exploiting the Bootstrap Loader (BSL) which enables writing and reading on the micro controller's memory. The adversary can also attack the external flash or EEPROM where sometimes valuable data are stored. A simple way to realize this attack is to eavesdrop on the conductor wires connecting the external memory chip with the micro controller. Another form of tampering attack can consist in replacing or injecting sensor nodes. In [5] the authors present new key management protocol that detect the injection of malicious nodes in the network. There is not a global solution against all these attacks. Standard precautions can be applied like disabled the JTAG interface or the use a good password for the bootstrap loader. Using the ontology, the intention of the tampering attack is to be authenticated and to be authorized in the network. The movement will be, as explained above high-tech material as technical capabilities to extract information, the contributors are generally laptops, the vulnerabilities are the non protected hardware component of sensors and the open environment where the nodes are deployed. Then the target is the hardware component of node, for example the EEPROM or the BSL. The layer used here is the same as the jamming attack, the physical layer. Finally, the result is, in this case, the entire damage of service in the network.

3.2 Attacks on Link layer

3.2.1 Collisions

In the collision attack, the adversary sends his own signal when he hears that a legitimate node will transmit a message in order to make interferences. In theory, causing collisions in only one byte is enough to create a CRC error and to cripple the message. The advantages of a collision attack compared to a jamming attack is the short power energy consumed and the difficulty to detect it (the only evidence of collisions attacks is incorrect message). In fact, such an attack can target specially the ACK control message causing an exponential back-off in some MAC protocol. All countermeasures that can be used against jamming attacks can be applied to collision attacks. Another solution is to use *Error correcting codes* [20] which are efficient in situation where errors occur on a limited number of bytes but this solution presents also an expensive communication overheard and additional processings. According to the ontology, first the intention of the collision attack is to exhaust the battery by using the channel of communication indefinitely. Then in the movement class, the attacker does not really need particular technical capabilities and it can be launched by anyone in the network, the vulnerability is the data integrity requirement and the layer used is the link layer. The target is general logical and can be at the same time against internal service like power management and against provided services, for example the communication service. Finally the result can be partial degradation if the attack is launched in certain region in the network or total degradation if the attack is applied in multiple precise locations in the network.

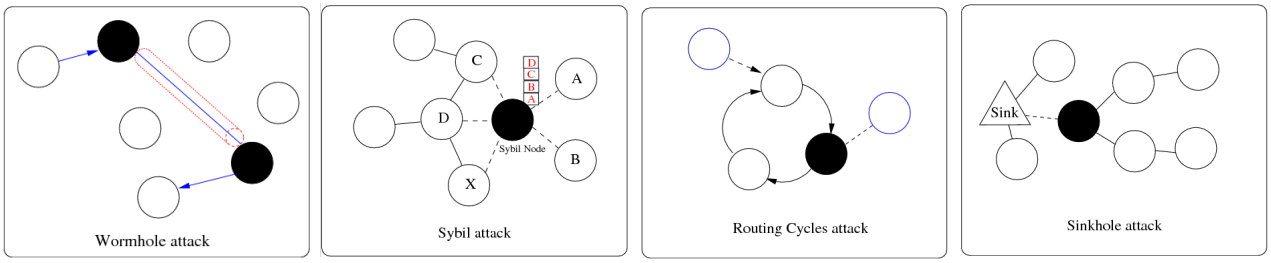
3.2.2 Exhaustion

Exhaustion attacks [16] consist in introducing collisions in frames towards the end of transmission and force the sensor node to retransmit continuously the packets until his death. This attack can be launched using a laptop or an ordinary sensor node. One way to defend against this attack is to limit the MAC admission control rate and so the sensor network can ignore excessive requests from the adversary and prevent energy loss. Another solution is to allow for each sensor node a small slot of time to access to the channel and transmit data, so it limits the possibility of long use of the MAC channel. The exhaustion attack present the same characteristics according to the ontology than the collision attack. The only difference is the vulnerability used where the exhaustion attack exploits the checksum fault of the transmitted message.

3.2.3 Link layer Jamming

In [17], the authors present a link-layer jamming attack. They mentioned that those jamming attacks are as effective as constant/deceptive/reactive jamming (explained in the jamming attack) and at the same time more

[1] JTAG is an IEEE 1149.1 standard designed to assist electronics engineers in testing their equipment during the development phase. Among other things, it can be used in current equipment for on-chip debugging, including single stepping through code, and for reading and writing memory. Many sensor nodes, as MICA2, Telos, ESB, have a JTAG connector on their circuit board allowing easy access to the micro controllers Test Access Port (TAP).



(a) (b) (c) (d)

Figure 2: Attacks on WSN.

energy-efficient than random or reactive jamming. The native idea is to find data packet and to jam it. But as they are generated spontaneously, it is very difficult to predict when data packets will arrive and then apply the attack. The solution proposed is to look at the probability distribution of the interarrival times between all types of packets. This attack was applied on three MAC protocols: S-MAC, B-MAC and L-MAC. The S-MAC probability distribution of packet interarrival times presents two separated clusters (denoted cluster1 and cluster2). This clear separation still stands even if we use mobile nodes or different data packet lengths. The attack exploits this particular phenomena. In fact if we have, for every cluster2 interarrival time, c cluster1 interarrival times, then right after observing a cluster2 interarrival time, we should expect c cluster1 interarrival times. So here the jamming attack becomes possible if we have an exact prediction model of packets arrival. The same idea could be applied to L-MAC protocol but the technique differs as it presents different probability distributions of packets interarrival times. Concerning B-MAC protocol, it is not possible to use the clusters idea as B-MAC use a periodic cycles only for listening and not for sending. The attack proposed in [17] against B-MAC first finds out the preamble check interval that the victim nodes are using and so has the possibility to launch jamming attacks. Moreover, the attack can take advantage of periodic listening to save energy. To prevent networks from this link layer jamming attack, some countermeasures are given. For S-MAC, the solution is to prevent clustering based analysis from being feasible. This can be done by narrowing the distance between the two clusters. In the case of L-MAC, a partial solution is to make the estimation of the clusters more difficult by changing the slot sizes (used for packet transmission) pseudorandomly as a function of time. For example a sensor node changes its packet slot size every second by picking a random value from a range. For the B-MAC, the only solution is to shorten the preamble in order to make its detection harder (the minimum value known is 10 ms). This link layer jamming attack was also studied on others slot-based MAC protocols (T-MAC [25], D-MAC [21]), frame-based protocols (PACT, Arisha [2], BMA [18], etc) and random access-based protocols (PCM [15], WiseMAC [10], etc). Using the ontology, here the intention is to disrupt communication. Moreover, it needs a very sophisticated radio to analyse the traffic and can be launched by one/many nodes or a laptop device. This attack exploits the propriety of data packets interarrival time at link layer level. The target of such attack is the communication services and the result is (like in the above attacks) a partial or total degradation of services in the network (depending on the region where the attacks is launched).

3.3 Attacks on Routing layer

3.3.1 Selective forwarding

In a selective forwarding attack [16], the malicious node forwards most messages and selectively drops, which means throwing away some of the data. One example of such attack is the black hole attack where the attacker chooses to drop all messages. The more the malicious node is closer to the base station, the more the attack is efficient (more traffic will pass through it). One way to mitigate this type of attack is to use multipath routing [11] in combination with random selection of paths to destination. These defenses lessen the probability that a message will encounter an adversary along all routes. Another solution is to use *monitor* nodes that ensure that their neighbors forward the messages. The use of watchdog can help this supervision. The intention of this attack is to alter data and loses a part of information (so it is a part of the unfairness category). Here the attack does not require any technical capabilities and can be executed by every node that participates in the routing mechanism. The vulnerability is that the message is not encrypted and anyone can read information in the packets. So it's clear that it use the routing layer. The target is generally the sink but can also be a sample

destination node. The result will be a total broken of all service offered by the network (for example wrong environmental alert) if we assume that all packets are altered.

3.3.2 Sinkhole

In the sinkhole attack [16], the malicious node tries to draw in all possible traffic. This is done by making the attacker very attractive to the surrounding nodes with respect to the routing metric (example higher power transmission). Then the surrounding nodes will choose the sinkhole node to route their data. For example, the Figure 2d shows the malicious node (black node) reacts like a sink and attracts all the traffic. One approach to avoid sinkholes is to use routing protocols [16] that verify the bidirectional reliability of a route with end-to-end acknowledgements which contain latency and quality information. The sinkhole attack's intention is to create a false sink and then create a false topology. It uses higher ressources to convince other nodes of its superiority. It is launched generally by a laptop or a PDA and it exploits the non authentication of links and identities. It is done at the routing layer level. The targets are all services provided by the network and the result is that information does not reach the base station, so it is a partial/total damage of the WSNs.

3.3.3 Sybil

In a Sybil attack [23] the malicious node assumes multiple identities. The goal is to fill a neighbouring node's memory with useless from non existing neighbours. For example, as some routing protocols use redundancy detection to eliminate sensor nodes, if a Sybil node assumes the identities of ten nodes, it can remove all this real neighbour nodes from neighbour tables of all nodes within its radio range. It can even remove the sink if the attacker presents a higher transmission's quality. In Figure 2b the malicious node forges and broadcasts the identities of nodes A, B, C and D for all its neighbors. As the identity fraud is the core of the Sybil attack, *authentication* is the key prevention against this attack, for example the SPIN algorithm [24] can be used. [9] shows that without a centralized authority, a Sybil attack is always possible. According to the ontology, the intention of the Sybil attack is included in the unfairness category by forging the identities of many nodes and so create information redundancy. This attack does not need any special technical capability and can be launched by one node or a laptop device. It uses the routing layer and exploits the non-authentication of node's identities. The target of such attack is always the provided services like data aggregation, voting, etc. The result of such attack can be partial or entire degradation of the network's service, depending on the location of the launch of the attack.

3.3.4 Hello flood

Many routing algorithms use hello packets to discover routes. In the hello flood attack [16], the attacker tries to convince all nodes to choose it as a parent using a powerful radio transmitter to bomb whole network with hello message announcing false neighbor status. So legitimate nodes will attempt transmission to the attacking node, despite many are out of range. If the attacker has the same reception capabilities, one way to avoid the hello flood attacks is to verify the *bi-directionality* of local links [16]. If not, *authentication* is a solution for nodes to verify the identity of theirs neighbors. Here, according to the ontology, the hello flood attack presents the same characteristics as the Sybil attack, but this attack needs a sophisticated radio to better diffuse the hello packets in the whole network.

3.3.5 Routing cycles

This attack [16] consists in making a path cycle between the source and the destination node. So the data message will go around in circles (figure 2c), possibly forever. This attack is simple to detect even by using tree-path routing protocols or using a hop count limit for forwarded packets. This attack presents also the same characteristics as the sinkhole attack but here the attack needs more than one attacker to create loops in the routing mechanism.

3.3.6 Wormhole

A wormhole attack [16] is a low-latency link between two nodes in the network which can be exploited by an attacker to apply other kind of attacks. This attack can be launched using an out-of-band or high-bandwidth channel between two malicious nodes, for example a direct wired link or a long-range directional wireless link. Figure 2a shows a situation where a wormhole attack takes place. We can also apply this type of attacks using

a singular malicious node where the attacker relays packets between two distant legitimate nodes to convince them that they are neighbors. Many defenses are given to prevent the wormhole attack as the use of packet leaches [13], MAD protocol [7], directional antennas [12], multi-dimensional scaling algorithm [26] and the use of Local Neighborhood Information [30]. Here the intention of the wormhole attack can be a passive eavesdrop of data, false topology creation or to be authenticated. It requires a very sophisticated radio or a cable to establish the long channel communication. It can be launched by at least two nodes or laptops at the routing layer. The targets are logical and the wormhole attack attempts to damage all services available in the network. the result is the same as the sinkhole attack.

Table 1: Summary of the ontology applied to WSN's attacks

Attack	**Ontology Attacks**						
	Intention	**Movement**				**Target***	**Result**
		Tech. Cap.	*Contri.*	*Vul.*	*Layer*		
Jamming	disrupt communication	radio	One/many, pc	Logical	physical	lps	Degra./broken
Tampering	Unfairness to be authenticated to be authorized	hitech	pc	hardware	physical	physical	Degra./broken
Collision	Unfairness	-	one/many, pc	logical	link	lis, lps	Degra./broken
Exhaustion	Unfairness	-	one/many, pc	logical	link	lps, lis	Degra./broken
Link layer jamming	disrupt communication	Radio	one/many, pc	logical	link	lps	Degra./broken
Selective forwarding	Unfairness	-	one/many, pc	logical	routing	lps	Degra./broken
Sinkhole	Unfairness	-	one/many, pc	logical	routing	lps	Degra./broken
Sybil	Unfairness	-	one/many, pc	logical	routing	lps	Degra./broken
Hello flood	Unfairness	radio	one/many, pc	logical	routing	lps	Degra./broken
Routing cycles	Unfairness	-	one/many, pc	logical	routing	lps	Degra./broken
Wormhole	Unfairness to be authenticated to be authorized	-	one/many, pc	logical	routing	lps	Passive/degra./broken
Flooding	Unfairness	battery	one/many, pc	logical	application	lis	Degra./broken
Desynchronisation	disrupt communication	-	one/many, pc	logical	application	lis	Degra./broken

*Target : lps = logical-provided services, lis = logical-internal services

3.4 Attacks on Application layer

3.4.1 Flooding

In this attack [27], the adversary tries to exhaust the memory and energy of a sensor node, which needs to maintain states at either end of connection, through flooding. The adversary will send successively requests to establish connection with a node until its death. This attack is similar to the TCP SYN attack where a node opens a large number of connections with another node to exhaust its resources. This attack can be realized with a simple sensor node or a laptop. The proposed solution to resist to this attack is the use of client puzzle. A connection will be only accepted after resolving a puzzle proposed by a server [3]. In general, puzzles are computationally expensive and hence serve as a deterrent to limit the rate request of the attacker. According the our ontology, the intention of such attack is to exhaust the limited ressources of nodes. It does not need any special materials but it needs a good battery. It can be launched by one/many nodes or a laptop and uses the application layers. The vulnerabilities used here is that there is no constraint on using network ressources or the authorization on modifying data packets. The target is the internal services of nodes such processing cycles and the result can be partial or total damages depends on the location of the attacks in the network.

3.4.2 Desynchronisation

This attack [27] consists on disrupting the existing connections among two nodes by resynchronizing their transmission. One way to apply this attack is to send repeatedly forged messages to the two nodes of the communicating parties with various fault flags like sequence and so to oblige them to go out of synchronisation. A simple defense consists in using an authentication mechanism to control the identity and the integrity of packets. The intention of such attack is to disrupt communication established between two legitimates nodes. It does not require special technical capabilities and also uses the application layer. The vulnerability that is exploited here is that sometimes we needs a radio synchronisation to communicate in the network. The target is internal services which are the requirement of synchronization in the appropriate layer. Finally the result consist in, as the flooding attack, a partial or total broken of network's services.

4 Conclusion

The paper presents a representative list of possible attacks and the associated defenses in a WSNs using a new ontology definition, summarized in table 1. We are now working on implementing this ontology, to enable an easier detection of such attacks in real cases if it is associated with an IDS system. The next step of our work is to validate the ontology by simulations and experiments on WSN.

References

[1] Edward G. Amoroso. *Fundamentals of computer security technology.* Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1994.

[2] K. Arisha, M. Youssef, and M. Younis. Energy-aware tdma based mac for sensor networks, 2002.

[3] Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo. DOS-resistant authentication with client puzzles. *Lecture Notes in Computer Science*, 2133:170+, 2001.

[4] A. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks, 2006.

[5] Chakib Bekara and Maryline Laurent-Maknavicius. A new protocol for securing wireless sensor networks against nodes replication attacks. *Wireless and Mobile Computing, Networking and Communications. WiMOB 2007. Third IEEE International Conference on*, pages 59–59, 8-10 Oct. 2007.

[6] Fatiha Benali, Véronique Legrand, and Stéphane Ubéda. An ontology for the management of heteregenous alerts of information system. In *The 2007 International Conference on Security and Management (SAM'07)*, Las Vegas, USA, June 2007.

[7] Srdjan Capkun, Levente Buttyán, and Jean-Pierre Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. In *SASN*, pages 21–32, 2003.

[8] Frederick B. Cohen. Information system attacks: A preliminary classification scheme. In *Computers and Security*, pages 29–46, 1997.

[9] J. Douceur. The sybil attack, 2002.

[10] A. El-Hoiydi, J.-D. Decotignie, C. Enz, and E. Le Roux. Poster abstract: wisemac, an ultra low power mac protocol for the wisenet wireless sensor network. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 302–303, New York, NY, USA, 2003. ACM.

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks, 2001.

[12] Lingxuan Hu and David Evans. Using directional antennas to prevent wormhole attacks. In *NDSS*, 2004.

[13] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In *INFOCOM*, 2003.

[14] David Icove, Karl Seger, and William R. VonStorch. *Computer crime: a crimefighter's handbook*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1995.

[15] E. Jung and N. Vaidya. A power control mac protocol for ad-hoc networks, 2002.

[16] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315, September 2003.

[17] Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel, and Paul Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 76–88, New York, NY, USA, 2005. ACM.

[18] Jing Li and Georgios Y. Lazarou. A bit-map-assisted energy-efficient mac scheme for wireless sensor networks. In *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*, pages 55–60, New York, NY, USA, 2004. ACM.

[19] Ulf Lindqvist and Erland Jonsson. How to systematically classify computer security intrusions. In *SP '97: Proceedings of the 1997 IEEE Symposium on Security and Privacy*, page 154, Washington, DC, USA, 1997. IEEE Computer Society.

[20] Hang Liu, Hairuo Ma, Magda El Zarki, and Sanjay Gupta. Error control schemes for networks: An overview. *Mobile Networks and Applications*, 2(2):167–182, 1997.

[21] G. Lu, B. Krishnamachari, and C. Raghavendra. An adaptive energy-efficient and low-latency mac for data gathering in sensor networks, 2004.

[22] Peter G. Neumann. *Computer related risks*. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1995.

[23] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268, New York, NY, USA, 2004. ACM.

[24] Adrian Perrig, Robert Szewczyk, Victor Wen, David E. Culler, and J. D. Tygar. SPINS: security protocols for sensor netowrks. In *Mobile Computing and Networking*, pages 189–199, 2001.

[25] Tijs van Dam and Koen Langendoen. An adaptive energy-efficient mac protocol for wireless sensor networks. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 171–180, New York, NY, USA, 2003. ACM.

[26] Weichao Wang and Bharat K. Bhargava. Visualization of wormholes in sensor networks. In *Workshop on Wireless Security*, pages 51–60, 2004.

[27] A.D. Wood and J.A. Stankovic. Denial of service in sensor networks. *Computer*, 35(10):54–62, Oct 2002.

[28] A.D. Wood, J.A. Stankovic, and S.H. Son. Jam: a jammed-area mapping service for sensor networks. *Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, pages 286–297, 3-5 Dec. 2003.

[29] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang. Jamming sensor networks: attack and defense strategies. *Network, IEEE*, 20(3):41–47, May-June 2006.

[30] Wassim Znaidi, Marine Minier, and Jean-Philippe BABAU. Detecting wormhole attacks in wireless networks using local neighborhood information. In *In IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Cannes, French Riviera, France, September 2008.

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399