Attack Detection vs. Privacy – How to Find the Link or How to Hide It?

Jiří Kůr, Vashek Matyáš, Andriy Stetsko, and Petr Švenda

Masaryk University, Brno, Czech Republic
{xkur,matyas,xstetsko,svenda}@fi.muni.cz

Abstract. Wireless sensor networks often have to be protected not only against an active attacker who tries to disrupt a network operation, but also against a passive attacker who tries to get sensitive information about the location of a certain node or about the movement of a tracked object. To address such issues, we can use an intrusion detection system and a privacy mechanism simultaneously. However, both of these often come with contradictory aims. A privacy mechanism typically tries to hide a relation between various events while an intrusion detection system tries to link the events up. This paper explores some of the problems that might occur when these techniques are brought together and we also provide some ideas how these problems could be solved.

1 Introduction

A wireless sensor network (WSN) consists of resource-constrained and wireless devices called sensor nodes. WSNs are considered for and deployed in various scenarios such as emergency response or energy management, medical, wildlife or battlefield monitoring. When deployed in an area, they monitor some physical phenomenon (e.g., humidity, temperature, pressure, light) and send measurements to a base station. Since the communication range of a sensor node is limited to tens of meters and the area of deployment is often large, not all sensor nodes can directly communicate with a base station and hence use hop-by-hop communication.

In WSNs, the risk of an attack happening is higher than in conventional networks, since the area of deployment is rarely protected physically. If an attacker captures some nodes, she becomes an authenticated participant of the network and can launch a variety of attacks. For an example of attacks, see [KW03]. The active attacks can be detected by a network intrusion detection system (IDS). Both centralized and distributed approaches can be applied. We believe that the distributed one is more reasonable in WSNs since it is more robust and less energy consuming. In this approach, every sensor node can run an IDS monitoring its neighbours and trying to detect an attack by itself or in cooperation with close neighbouring sensor nodes. We do not assume that every sensor node runs an IDS, although this would be possible. Further in the paper, when we mention an IDS we mean one IDS (instance) running on a certain node. Nevertheless, a centralized IDS is also worth considering in the future.

B. Christianson et al. (Eds.): Security Protocols 2011, LNCS 7114, pp. 189–199, 2011.

However, an IDS is usually inadequate for defending the network against a passive attacker, who quietly monitors the network communication. This type of attacker may infer sensitive information in the presence of packet encryption using traffic analysis techniques. Sensitive information leaked by traffic patterns may include location of certain nodes and events, movements of monitored subjects, frequency of events, location of a base station, etc. Thus privacy mechanisms, e.g., obfuscating the traffic patterns, should also be included in the defence line of WSNs.

It seems natural to employ both IDSs and privacy mechanisms to protect a WSN yet they have contradictory aims as we shall see. The aim of an IDS is to detect an attack and preferably to identify/eliminate the source of the attack. Detection accuracy of an IDS often depends on its ability to link certain events, e.g., packet X was sent by node Y and received by node Z. When privacy mechanisms are enabled, the IDS ability to link certain events is likely to decrease – implying a decrease in its detection accuracy.

The aim of this paper is to find out whether it is possible to use both IDSs and privacy mechanisms in WSNs at the same time, and how they might influence the functionality of each other. We focus on this conflict only within WSNs since these networks differ from other environments w.r.t. some important aspects for both IDSs and privacy mechanisms – energy and communication constraints, processing power, etc.

The roadmap of this paper is as follows – in Section 2, we first present several problems that may appear when both IDS and privacy mechanisms are employed in the network. In Section 3, we discuss possible approaches to mitigate these problems. Section 4 sketches details of possible solutions to some of the problems, and the following section then concludes the paper.

2 Possible Problems

In this section, we present problems that might occur when both IDSs and privacy mechanisms are used simultaneously. These problems are divided into four categories based on the cause and nature of the problems. Subsection 2.1 discusses problems within the first three categories, concerning issues that privacy mechanisms may cause to IDSs. The last category, concerning problems that IDSs may cause to privacy mechanisms, is then discussed within Subsection 2.2. The problems are denoted with Roman numbers, with continuous numbering throughout the following subsections.

2.1 Problems that Privacy Mechanisms May Cause to IDSs

Multiple or hidden identities. Privacy mechanisms usually intentionally hide the identity of nodes, assign multiple pseudonyms to a single node or use dynamically changing pseudonyms [MX06]. Thus a single node may have different pseudonyms for communication with different neighbours and these pseudonyms may change in time. Packets sent by the node then contain identifiers that are

understandable only to this node and the intended recipient. This may cause trouble to an IDS since it is not able to link overheard packets with a particular sender or recipient. The IDS will also not be able to decide whether the claimed pseudonym of a node is true or not. Let us consider the following problems:

I An IDS concludes that a particular node is malicious. However, it may not be able to mark the node as malicious since it has no suitable identifier of the node that could be unambiguously understood by other nodes. Thus it will have trouble providing other nodes with the information that the certain node is malicious. A usual way to cope with this problem is to use the physical location of the malicious node. However, the nodes may only have some information on the radio signal strength of the attacking node received packets, not its accurate location.

II An IDS may not be able to detect a Sybil attack [KW03] since it is legitimate for every node to have multiple identities. An IDS without additional information is not able to distinguish between a true identity and a malicious identity either fabricated or stolen.

III Detection accuracy of an IDS may decrease if it does not know the identities of its neighbours. For example, in order to detect a selective forwarding attack an IDS (running on the node A, see Figure 1 below) monitors packets in its communication range. If the IDS overhears a packet (from the node X), it may want to check whether the packet is properly forwarded by the recipient (the node Y). If the IDS assumes that the recipient is in its communication range, while it in fact is not, false positives might occur. On the contrary, if the IDS assumes the recipient is out of reach and it is not true, false negatives might occur.

IV An IDS may not be able to detect a selective forwarding (jamming) attack in case a forwarding (jamming) node has multiple identities and the IDS does not know that these identities belong to that node. Then the IDS cannot link two dropping (sending) events that look innocent when separated and

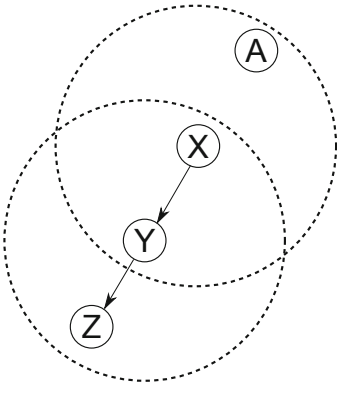

Fig. 1. The node A does not know whether the recipient (node Y) is in its communication range

would be recognized as an attack when linked together. Furthermore, the IDS has to maintain larger tables in the memory due to a higher number of identities monitored.

Randomized sending rate and route diversity. Attacks are usually detected by monitoring the sensor nodes behaviour [OM05, KDF07, LCC07, SFM10], e.g., packet sending rate, packet dropping rate, received packet signal strength. When privacy mechanisms modify network behaviour of sensor nodes in order to decorrelate traffic patterns, an IDS might have problems to differentiate legitimate and malicious behaviour.

V Privacy mechanisms may use dummy packets to suppress traffic patterns [OZT04]. A node introducing a dummy packet or dropping a dummy packet may be considered malicious by an IDS. On the contrary, if such behaviour is tolerated, a malicious node can introduce malicious or drop legitimate traffic without being detected.

VI Privacy mechanisms may route data through multiple different and randomly chosen routes [OZT04]. Thus, an IDS does not get a steady flow of packets to analyze.

VII An IDS monitors other nodes for packet dropping by checking if an incoming packet is resent in a reasonable time frame [SFM10]. Privacy mechanisms that will use some kind of anonymity mixing technique [HWK+05] will interfere with such detection, because a packet may be delayed for some time (therefore increasing the detection window that needs to be tolerated on IDS's side).

VIII Honest nodes may intentionally imitate the behaviour of a base station (BS) to hide the location of the true BS [BMM07]. These nodes may be then considered malicious by an IDS. On the contrary, if such behaviour is tolerated by IDSs, a malicious BS may remain undetected.

Encryption and changes of packet appearance. Privacy mechanisms usually employ packet encryption to hide the content of packets or to change the packet appearance hop-by-hop [SGR97, DHM04].

IX If encryption is used and an IDS does not posses appropriate keys, it cannot analyze packet content.

X If privacy mechanisms use some kind of hop-by-hop or onion encryption, an IDS without encryption keys is not able to decide whether the forwarded packet corresponds to the received one. Then a malicious neighbour would be able to modify packets in an undetected manner or to drop original packets and send dummy ones instead.

2.2 Problems That IDSs May Cause to Privacy Mechanisms

Not only privacy mechanisms cause trouble to an IDS, also the IDS can negatively influence privacy mechanisms.

XI Privacy mechanisms may decrease the relevant anonymity set by excluding potentially compromised or misbehaving nodes detected by an IDS. An attacker may influence the IDS decisions and therefore indirectly influence the privacy mechanism. Cooperation between an IDS and a privacy mechanism actually opens new attack vectors.

XII IDS traffic or decisions may leak sensitive information on node identities or relations between nodes. Privacy mechanisms thus also have to take care of the IDS traffic.

3 Towards a Successful Cooperation of IDSs and Privacy Mechanisms

We have presented several problems that may arise when privacy mechanisms and IDSs are employed together, though we believe that they can successfully coexist and even cooperate. We do not aim to discuss possible solutions in their entirety at this stage, we shall provide the necessary details of selected solutions in the Section 4. The following approaches may be adopted.

3.1 Both Privacy Mechanisms and IDSs Are Designed in a Non-interfering Way and Still Achieve Their Goals

The simplest way to avoid all of the aforementioned problems is to run protocols that do not cause these problems. However, the likely cost for this evasion will be a decrease in performance (security functionality) of either IDSs, privacy mechanisms or both. Another impact can be an increase in protocol complexity. For example, the IDS may use a node behaviour to identify this node (see Problem I) instead of the node identifier. Such behaviour may be represented by hashes of messages sent by the node recently. This information can be understood by all nodes in the communication range of the malicious one.

3.2 Privacy Mechanisms and IDS Cooperate

Privacy mechanisms "make a mess" in a network by hiding identities of nodes, introducing new traffic, etc. Privacy mechanisms might share some (secret) information with an IDS, in particular should this sharing help the IDS to "organize the mess" and successfully detect active attackers. A problem to solve is that a certain IDS node may accumulate a lot of secret information, becoming a sweet spot for an attacker.

1. **Pre-shared secret.** Privacy mechanisms employ a trapdoor function for pseudonym generation, content protection or dummy traffic identification. The trapdoor information is pre-shared between a privacy mechanism and an IDS, thus the IDS knows all the information necessary to run properly. No further cooperation is needed. However, the IDS knowing the trapdoor information is tempting for an attacker. The impact of an IDS compromise can be minimized by sharing only partial information or information that is valid only for a certain time.

2. **Delayed information disclosure.** Certain information is retrospectively revealed by privacy mechanisms, especially if this information helps the IDS to understand audit data recorded in the past. This approach assumes that an attacker needs the information immediately and delayed disclosure is not helpful for her. This approach can be used, for example, to retrospectively differentiate dummy and real traffic w.r.t. Problem V.
3. **Information is revealed on demand.** The information necessary to cancel the effect of privacy mechanisms' protective actions can be obtained by an IDS on demand, if the IDS executes an additional protocol and a privacy mechanism cooperates. The key characteristics are that IDSs cannot obtain the information without cooperation of privacy mechanisms and the obtained information is limited to cancelling effects of privacy mechanism protective actions only for a certain subject or time period (one message, one identity, etc.).
4. **Threshold scheme for information availability.** Information available to an IDS running on a particular node is intentionally limited to provide additional resilience against the node compromise. To obtain full information required, multiple nodes with an IDS/privacy mechanism must cooperate, potentially with the support of a suitable cryptographic threshold scheme.

3.3 Involvement of a Trusted Third Party

Another option to solve problems between privacy mechanisms and IDSs is to introduce a trusted third party, which will possess all necessary information to resolve the problems. E.g., Problem VIII could be solved by cooperation with a real BS. The BS could grant a ticket to a particular node to act as a BS. This node can later broadcast this ticket to its neighbours, so that the IDSs are sure that this node is either the real BS or a legitimate node imitating the BS.

3.4 IDSs and Privacy Mechanisms Leverage Properties of Each Other

Co-existence of IDSs and privacy mechanisms may benefit both when used properly. If an IDS has several identities, it can, for example, send a probing message (using one identity) that should be forwarded back to itself (represented by another identity). These probing messages increase the amount of traffic and may play the role of dummy traffic. This also makes the traffic analysis harder and helps the privacy mechanism. Another benefit is that an attacker cannot easily avoid an IDS by selecting one (static) path without IDSs if a privacy mechanism ensures that multiple routes or randomly chosen routes are used.

4 Sketching Some Solutions

The problems described in Section 2 can be solved to some extent by approaches suggested in Section 3. The details of a particular solution are usually dependent on many parameters of the protected network and requirements on IDSs

and privacy mechanisms. Here, we will provide a more detailed outline of the techniques from Subsection 3.2 with their demonstration on a common privacy scheme and an IDS. The goal is *not* to provide a detailed new scheme for co-operation of IDSs and privacy mechanisms, but rather to provide an evidence that the techniques from Subsection 3.2 are not completely theoretical and can be used in the context of existing schemes.

4.1 How to Hide a Link

A privacy mechanism can operate in various modes that offer different levels of privacy protection. For example, the privacy mechanism can hide:

- both sender and recipient identities;
- either sender or recipient identity;
- neither of them.

We consider and describe a privacy mechanism operating in the mode when sender and recipient identities are hidden, which is the worst mode for the IDS. The chosen example mechanism is based on commonly accepted principles and assumes a network where each sensor node has a unique identifier that is known to all the neighbours. Instead of using the unique identifiers X and Y (see Figure 2), the node X generates a new pseudonym every time it sends a new packet to the node Y. Based on the pseudonym, only the recipient Y knows that the packet is addressed to it and that the packet comes from the node X. An instance of such privacy mechanism can be found in [MX06].

The pseudonym generation can be done in various ways. In order to present the ideas from Subsection 3.2, we consider two schemes both of which assume that any two communicating nodes share a pairwise key K_m:

- *Scheme 1* – The sender X directly uses the pairwise key K_m to create pseudonyms, for example, by encrypting a counter using the key. The counter increases every time a new packet is sent to the recipient Y.
- *Scheme 2* – The sender X does not use the pairwise key K_m directly to create pseudonyms. Instead, it uses the key to derive n session keys. Every session key is then used to create a limited number of pseudonyms. Note that this scheme applies common security principle of short-time-secret derivation that limits the master secret usage.

Both alternatives of the privacy mechanism cause the following problems to an IDS that runs on the node A (see Figure 2):

- It cannot deduce that all three packets were sent by the same node X and all of them were addressed to the same node Y. Thus Problems II, III and IV arise.
- It cannot decide what traffic must be logged and what traffic can be left out, which leads to the storage memory problem (see Problem IV).
- It cannot decide whether the packets were forwarded or not (see Problem IV). For example, if the node Y encrypts the content of the packets received from the node X and forwards them to the node Z using other pseudonyms (P_{21}, P_{22} and P_{23} as depicted on Figure 2).

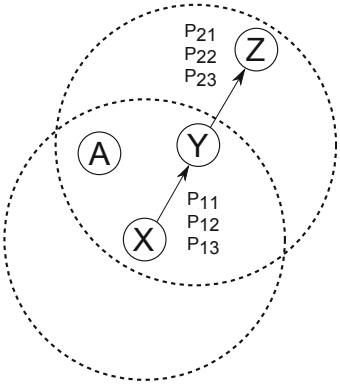

Fig. 2. The node X sends three packets to the node Y using three different pseudonyms P_{11}, P_{12} and P_{13}. The node Y forwards the received packets to the node Z using other pseudonyms P_{21}, P_{22} and P_{23}.

4.2 How to Find a Link

The problems previously described can be solved by adopting approaches sketched in Subsection 3.2. Note that in both the schemes the pseudonyms are generated using a trapdoor information, namely the pairwise key in the *Scheme 1* and the session key in the *Scheme 2*. Hence if the IDS has access to this trapdoor information, it can effectively uncloak the pseudonyms. This access can be granted by the following methods:

Pre-shared secret – full disclosure. Nodes X and Y pre-share the pairwise key K_m also with the IDS. This enables the IDS to uncloak the pseudonyms and analyze the traffic in realtime. This solution is straightforward, efficient and works for both the *Schemes*, yet it suffers from several drawbacks. The IDS becomes a sweet spot for an attacker as it is able to uncloak all the pseudonyms and even impersonate nodes in the neighborhood. The problem escalates if an IDS is running on every node.

Pre-shared secret – partial disclosure. The drawbacks of the full disclosure can be mitigated by pre-sharing only *partial information* that is valid only for a certain time period or a certain number of messages. When the *Scheme 2* is in use, the nodes X and Y pre-share with the IDS only a limited number of session keys and thus limit the information available to the IDS. A tradeoff rule applies: the more information is shared, the more accurate the detection and the worse the impact of a potential IDS compromise is.

Note that the *Scheme 2* can be particularly useful if every node runs an IDS. Each node may then possess different session keys. So every pseudonym can be uncloaked by some IDS, but there is no IDS that has access to all of them.

Delayed information disclosure. To partially avoid problems with pre-sharing, the trapdoor information may be disclosed to the IDS retrospectively.

In the case of *Scheme 2* the session keys would be shared with the IDS once they become obsolete. This is very useful in situations when the communication has to be protected only during a certain short time period. After this period the used session keys can be shared or even made public, because the protected information is obsolete. Yet the fact that a certain node is malicious may be important even with a short delay. Furthermore, the delayed session key disclosure does not enable anyone to forge the pseudonyms.

A drawback of the delayed disclosure is that the IDS has to maintain a log of past traffic and is not able to analyze it until the session key is revealed. Thus the detection of malicious activities (if present) is delayed and requires more storage memory.

The delayed disclosure of information is not limited only to the disclosure of the session keys. Each IDS may control only partial trapdoor information and these pieces can be put together only at a certain time or after a certain event. Thus an attacker that has compromised only a fraction of the IDSs does not gain access to the complete trapdoor information prior to its delayed disclosure.

Information is revealed on demand. The trapdoor information can be disclosed on demand. This method may combine pre-sharing with delayed information disclosure. The time of the disclosure and the type of the disclosed information is specified by the IDS which requests the information. Yet the decision whether to fulfil the request or not (e.g., based on the previous requests) is left to the owner of the information.

Assume the *Scheme 2* is in use. In order to analyze the traffic, the IDS needs to gain access to the session keys. So it requests the session keys from the nodes X and Y when necessary. Depending on the IDS, it may request past, current or even future session keys. However, in all the cases it should be able to make only a limited number of such requests. This limitation is vital as it prevents the IDS from accessing all the session keys in case the IDS is compromised. A drawback of the limitation is that a misbehaving node has a chance to cheat and remain undetected since the IDS cannot ask for and uncloak all the pseudonyms. Note that the limitation on requests sets the security tradeoff – the more requests are allowed, the more accurate the detection and the worse the impact of a potential IDS compromise is.

5 Conclusion and Further Work

We explored some of the problems that might occur when both intrusion detection systems and privacy mechanisms are employed in wireless sensor networks at the same time. Problems with an intrusion detection system might occur when a privacy mechanism changes packet appearance, hides identities of nodes or changes a network traffic pattern. On the other hand, an intrusion detection system may leak sensitive information or enfeeble a privacy mechanism. We provided some ideas on how these problems could be solved. We demonstrated that some of these ideas can be applied in the context of existing schemes. Yet some of them still await a deeper examination.

We encountered several open issues that are worth exploring in the future. We highlighted only the most promising ones – from our point of view. We plan to explore the threshold schemes for information availability in a greater detail. Furthermore, we would like to examine solutions involving a trusted third party. Yet such solutions need to be efficient and without any significant communication overhead – and this will be a tricky task. Another issue arises with the on-demand information disclosure. This approach requires an anonymous scheme for limiting the number of requests an IDS can make. Finally, we would like to investigate the issues of active probing/testing, where an IDS may actively probe suspicious nodes by sending them probing messages. Such probing need to be done in an efficient and preferably anonymous way.

Acknowledgement. We are grateful to our colleagues from the Laboratory of security and applied cryptography, namely Filip Jurnečka, Marek Kumpošt, Marián Novotný, Zdeněk Říha, Tobiáš Smolka and Roman Žilka for the discussions and suggestions that improved the paper.

This work was supported by the project GAP202/11/0422 of the Czech Science Foundation. Jiří Kůr and Andriy Stetsko were additionally supported by the project GD102/09/H042 "Mathematical and Engineering Approaches to Developing Reliable and Secure Concurrent and Distributed Computer Systems" of the Czech Science Foundation.

References

[BMM07] Biswas, S., Mukherjee, S., Mukhopadhyaya, K.: A countermeasure against traffic-analysis based base station detection in WSN. In: Web Proceedings of the International Conference on High Performance Computing, HiPC 2007 Posters, poster session (2007)

[DHM04] Deng, J., Han, R., Mishra, S.: Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks. In: DSN 2004: Proceedings of the 2004 International Conference on Dependable Systems and Networks, pp. 637–646. IEEE Computer Society, Washington, DC, USA (2004)

[HWK+05] Hong, X., Wang, P., Kong, J., Zheng, Q., Liu, J.: Effective probabilistic approach protecting sensor traffic. In: IEEE Military Communications Conference, MILCOM 2005, vol. 1, pp. 169–175 (October 2005)

[KDF07] Krontiris, I., Dimitriou, T., Freiling, F.C.: Towards intrusion detection in wireless sensor networks. In: Proceedings of the 13th European Wireless Conference (2007)

[KW03] Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127 (2003)

[LCC07] Liu, F., Cheng, X., Chen, D.: Insider attacker detection in wireless sensor networks. In: Proceedings of the 26th IEEE International Conference on Computer Communications, pp. 1937–1945 (2007)

[MX06] Misra, S., Xue, G.: Efficient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks 1(1), 50–63 (2006)

[OM05] Onat, I., Miri, A.: An intrusion detection system for wireless sensor networks. In: Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, pp. 253–259 (2005)

[OZT04] Ozturk, C., Zhang, Y., Trappe, W.: Source-location privacy in energy-constrained sensor network routing. In: SASN 2004: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 88–93. ACM, New York (2004)

[SFM10] Stetsko, A., Folkman, L., Matyas, V.: Neighbor-based intrusion detection for wireless sensor networks. Technical Report FIMU-RS-2010-04, Faculty of Informatics, Masaryk University (May 2010)

[SGR97] Syverson, P.F., Goldschlag, D.M., Reed, M.G.: Anonymous connections and onion routing. In: Proceedings of IEEE Symposium on Security and Privacy, 1997, pp. 44–54 (May 1997)