Requirements for wireless sensor networks in order to achieve digital forensic readiness

Francois Mouton and Prof Hein Venter

Man's pursuit of a better lifestyle has led to a vast improvement in technology. Wireless sensor networks (WSNs) have been developed to improve our ability to accomplish daily tasks. The implementation of security protocols on WSNs has not received much attention to date and very little consideration has been given to digital forensics in a WSN environment.

There is currently no formal set of requirements for achieving digital forensic readiness in a WSN.

Wireless sensor networks

WSNs belong to the general family of sensor networks that use multiple distributed sensors to retrieve data from various environments. A WSN is defined as an ad hoc wireless network that consists of tiny and resilient computing nodes known as motes or sensors. These motes are extremely efficient in terms of power consumption and collaborate effectively with other motes in their vicinity.

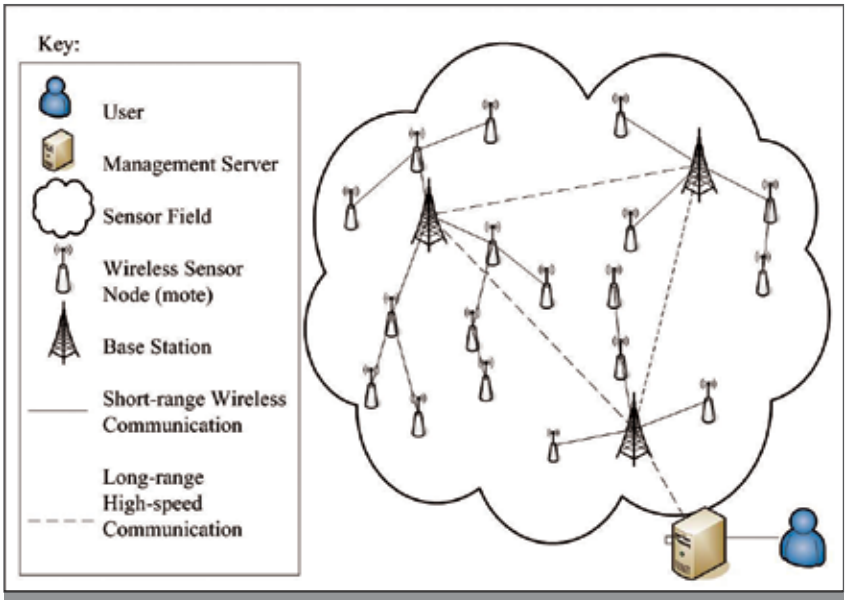

Figure 1: A graphical representation of a WSN (Mouton & Venter, 2009)

Table 1: A graphical representation of a WSN (Mouton & Venter, 2009)

WSN component	Functions of each component
User	The user can interact with the WSN through the management server.
Management server	The management server serves as an interface console for the WSN.
Sensor field	The sensor field denotes the physical boundaries of the WSN.
Wireless sensor node (mote)	Each mote contains a small subset of the various sensors. Motes in the network can also act as repeaters for packets that need to reach the base station.
Base station	A base station serves as a gateway node through which the information of the motes has to travel to reach the management server.
Short-range wireless communication	Short-range wireless communication links are established between neighbouring motes and the neighbouring base stations.
Long-range high-speed communication	Long-range high-speed communication links are established between further-ranged base stations and the management server.

WSNs can be used in many environments. Their motes may consist of many different types of sensors, such as thermal, visual, infrared, radar or acoustic. These motes can monitor a variety of ambient conditions, including humidity, pressure, sound, noise levels, temperature, lighting conditions and objects moving through a designated area (Elson & Estrin, 2001; Kahn et al., 1999).

Digital forensic readiness

Tan (2001) identifies two objectives that have to be balanced carefully: maximising the ability to collect credible digital evidence, and minimising the cost of performing a digital forensic investigation. Even though these objectives provide a good definition of digital forensic readiness, it is important to refine them to make them more specific to a WSN environment.

For the purpose of this article, digital forensic readiness is defined as performing a digital forensic investigation in the shortest time with the lowest cost, without disrupting the original network that has to perform mission-critical tasks.

Differences between WSNs and WLANs

Wireless sensory networks have special needs and have more specialised requirements than wireless local area networks (WLANs). There are many factors that distinguish a WSN from a WLAN, including the following:

- Communication protocol
- Proof of authenticity and integrity
- Time stamping
- Modification of the network after deployment
- Protocol data packets

While examining each of these factors, the authors assume that no modification to the original WSN (oWSN) is allowed and a secondary independent forensic WSN (fWSN) would be used for the digital forensic readiness implementation of the oWSN.

Communication protocol

All communication within a WSN occurs in a broadcast fashion and a mote never really knows which of its neighbouring motes actually receives the packet (Akyildiz et al., 2002; Tseng et al., 2003). The default functioning of a mote in the sensor field is to listen for all packets. Upon receipt of a packet, it has to analyse if the packet was meant for it or not. This analysis requires some processing that drains the battery of the mote.

The broadcasting technique used in WSNs is very different from the communication techniques used in IEEE 802.11x wireless networks. In the WLAN environment, one can always determine if a packet has arrived at its destination by monitoring the network (Xylomenos & Polyzos, 1999; Xylomenos et al., 2001). This is not the case in a WSN environment.

Due to the broadcasting fashion in which WSNs communicate, the mote that broadcasts packets will never be completely sure whether the packet was received by the correct mote. This uncertainty could be overcome by a communication protocol that allows the receiving mote to reply with a receipt acknowledgement packet. If a flooding attack is launched against the oWSN, it would compel the oWSN to reply to each flooding attempt with receipt acknowledgement messages.

Proof of authenticity and integrity

Considering that it can have a severe impact on a WSN environment, it is impractical to use a protocol founded on receipt acknowledgement packets. In the case of the fWSN, this problem could be avoided by implementing a protocol that uses receipt acknowledgement packets, because it is in the nature of a forensic network to always be sure that the information received at either point of the communication line contains some degree of authenticity and integrity. In order to achieve sound digital forensic readiness, it is crucial to prove the authenticity and integrity of the data packets that have been received. In the context of this article, authenticity is the certainty that the origin and intentions of the data packet are kept intact throughout its lifetime. Integrity is defined as the certainty that the correctness of the data in the data packet is kept intact throughout the lifetime of the data packet.

Firewalls and wireless routers are examples of equipment that could be found in an IEEE 802.11x wireless network. Most of these devices can generate a log or some other way of showing which data packets have passed through the network. This log file can also be backed up by looking at all the other devices through which this single packet has travelled.

In a WSN environment, very little or no logging is done on the motes in the sensor field. WSN equipment, by default, only does logging at the base station. Because WSNs differ so significantly from WLANs, a form of logging that is based on the Casey Certainty Scale (Casey, 2002) is proposed.

Fortunately, in a WSN environment, multiple motes tend to be able to capture the same data packet simply because they are all in range of a particular broadcasted packet. This is a feature of WSNs, which is not the case in IEEE 802.11x networks. Most devices in WLANs will ignore packets that are not meant for them and do not even attempt to log these packets. The opposite is true for WSNs, where motes attempt to capture every data packet within range. This feature of WSNs can be exploited in an attempt to prove the authenticity and integrity of packets in the WSN. All the packets captured by each independent fWSN mote could be forwarded to the base station, as a central point of analysis, in an effort to prove the authenticity and integrity of the data packet.

According to Casey (2002), the integrity and authenticity of information is more certain if it was recorded by different independent sources. Each mote can be seen as an independent source and the authenticity and integrity of each packet can be determined, based on the number of motes in the network that have received the same broadcasted packet.

This article assumes that a packet that has been seen by a larger number of motes has far greater authenticity and integrity than a packet that has only been seen by a few forensic motes in the network.

Time stamping

Time stamping in a WLAN environment is a fairly easy task, since all the devices in a WLAN would, under normal conditions, either have access to a time server or have been set to the correct time. Thus, time stamping in the logs for a WLAN would, under most conditions, be correct, provided that the device has not been tampered with or is not faulty. In the case of a WSN, however, only the management server (which is connected to the base station) has a sense of time. The only measurement the motes in a WSN environment can use is their own sense of time, which is the time that has elapsed since they were switched on (Sundararaman et al., 2005; Su & Akyildiz, 2005; Sun et al., 2006). This uptime is a poor indication of time, because all motes in the entire network have to be switched on simultaneously.

It was noted that it takes at most one second to capture any data packet and transmit it to the fWSN base station. This introduces a time delay between capturing a packet and receiving it at the base station. The time delay also differed according to the distance of the fWSN mote from the base station in terms of hops and physical distance. The time stamps at the base station are not an accurate reflection of when the packet was initially captured, as the base station is the only device that can assign an accurate time stamp if it is connected to the management server. It is also important to note that each fWSN mote captures packets sequentially, which means that even if the time stamps are altered, the sequence would still be intact.

The sequence of the data packets is not altered, and this (rather than the time stamps) could be used to verify the authenticity and integrity of the data packets. More information can be gathered by looking at the sequence of the data packets than by looking at their time of transmission.

It is therefore sufficient to capture the data packets and merely provide a time stamp for them as soon as they arrive at the fWSN base station. In the event that this is done, one would create a time stamp error (a constant error for each oWSN mote respectively), as it would reflect the time the data packet was first transmitted together with the added time it took for this data packet to reach the fWSN base station.

The time stamp error stays constant for all the packets received from a specific mote in the sensor field, so it is still possible to guarantee the authenticity and integrity of a packet. This constant error could be measured, if needed, by comparing the time stamps at the oWSN base station and the fWSN base station. The time stamp, combined with the sequence of the data packets, would then be used in a forensic investigation.

→ *Table 2: Requirements for achieving digital forensic readiness*

Requirements for achieving digital forensic readiness in an IEEE 802.15.4 WSN environment	
Communication protocol	1. The fWSN should use a receipt acknowledgement packet protocol to ensure that all data packets captured by the motes in the field reach the base station.
	2. The broadcasted communication from the oWSN should be intercepted in a manner that ensures that the data packets are not altered in any fashion.
	3. The fWSN should be able to capture all possible types of communication that can be sent from the oWSN.
Proof of authenticity and integrity	4. The authenticity and integrity of all the data packets should remain intact while being captured on the fWSN.
	5. The data packets that are captured on the fWSN should be stored in such a way that their authenticity and integrity are not compromised.
	6. It should be possible to verify the authenticity and integrity of all the data packets in case a digital investigation takes place.
Time stamping	7. The data packets should have a time stamp that does not violate their authenticity and integrity.
	8. The sequence of the packets captured should reflect the true sequence in which they were transmitted from the original network.
Modification of the network after deployment	9. It should be possible to implement the fWSN without any modification of the oWSN.
Protocol data packets	10. The fWSN should be designed in such a manner that the network topology or the routing protocol used by the oWSN does not influence the fWSN's operation.
Radio frequencies	11. The fWSN should be able to communicate on the same radio frequencies that are available to the oWSN.
	12. All communication within the fWSN should occur on a frequency not utilised by the oWSN.
	13. If an intruder WSN is in the area and communicates on a frequency that influences the oWSN, then the fWSN should be able to forensically capture these data packets.
Power constraints	14. The fWSN should not increase power consumption in the oWSN and the fWSN should have at least the same or a longer network lifetime than the oWSN in terms of battery power.
Network overhead	15. While intercepting communication, there should be no extra network overhead on the oWSN.
Data integrity	16. The fWSN should by no means be able to influence the oWSN or influence any sensory data transmitted within the oWSN.

Modifying the network after deployment

The ability to modify the network after deployment is the only factor that is fairly similar between WLANs and WSNs, as it is always possible to modify the code on a device by retracting it from the field, re-developing it and then redeploying it.

However, the practicality of altering oWSN devices after deployment must be considered. It is important to remember that oWSN motes are usually scattered in an area and to alter them, one would have to collect the entire network and redeploy it.

The difficulty and impracticality of modifying the oWSN led the authors to believe that this should also be seen as a specific requirement when attempting to provide forensic readiness to a WSN environment.

Considering that one cannot easily alter the oWSN, one must ensure that the fWSN is able to handle any type of protocol headers and footers that could originate from the oWSN.

Protocol data packets

The oWSN can have different types of communication protocols in its normal operation. The data packets can include packets to determine the routing protocol, sensory packets, encrypted packets or even malformed packets. To ensure that all the possible protocols used in WSNs are encapsulated in this approach, it is assumed that the oWSN uses an address-free protocol, which generates the largest amount of network overhead in WSNs, as it would cause data to be sent from a source mote in the network to every other mote in the network on each data transmission.

The most common address-free protocols are data dissemination protocols, where neither the sender mote nor any of the other motes in the network know the address of the receiving mote. If the fWSN is able to successfully log this communication of an address-free protocol in a way that ensures authenticity and integrity, one could assume that the name-based WSN protocols would effortlessly be accounted for, as they have much less network overhead (Dunkels et al., 2007).

As is also the case in WLANs, the motes in the fWSN should listen in promiscuous mode and should be able to handle any type of packet that is transmitted or received by the oWSN. Promiscuous mode is a configuration of the WSN mote in which all traffic within the WSN mote's frequency range and wireless range will be received by the WSN mote. If an attacker uses a foreign mote to inject data into the oWSN, the fWSN should also be able to listen in on this data.

The fWSN should be using a name-based WSN protocol for communication between other fWSN motes, as it is more effective than address-free protocols in terms of network overhead. In name-based protocols, the source mote knows the address of the receiving mote and the motes between the sender and receiver know the path to the receiving mote (Dunkels et al., 2007).

Forensic readiness requirements for WSNs

A list of requirements is thus proposed that need to be taken into consideration when implementing digital forensic readiness for an IEEE 802.15.4 wireless sensor network. Table 2 summarises the important requirements that need to be taken into account in order to achieve digital forensic readiness in an IEEE 802.15.4 WSN environment.

References

Akyildiz, IF, Su, W, Sankarasubramaniam, Y and Cayirci, E. 2002. Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422.

Casey, E. 2002 Error, Uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, 1(2), Summer.

Dunkels, A, Osterlind, F and Zhitao, H. 2007. An adaptive communication architecture for wireless sensor network. In: *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems, Sydney, Australia*, 335–349.

Elson, J and Estrin, D. 2001. Time synchronization for wireless sensor networks. In: *Proceedings of the 15th International Symposium on Parallel and Distributed Processing*, 1965–1970.

Kahn, JM, Katz, RH and Pister, KS. 1999. Next century challenges: mobile networking for "Smart Dust". In: *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, New York*, 271–278.

Mouton, F and Venter, HS. 2009. A secure communication protocol for wireless sensor networks. In: *Proceedings of the Annual Security Conference: Security Assurance and Privacy: organizational challenges, Las Vegas.*

Su, W and Akyildiz, IF. 2005. Time-diffusion synchronization protocol for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 13(2):384–397.

Sundararaman, B, Buy, U and Kshemkalyani, AD. 2005. Clock synchronization for wireless sensor networks: a survey. *Ad Hoc Networks*, 3(3): 281–323.

Sun, K, Ning, P and Wang, C. 2006. TinySerSync: secure and resilient time synchronization in wireless sensor networks. In: *Proceedings of the 13th ACM conference on computer and communications security, Alexandria*, 264–277.

Tan, J. 2001. *Forensic readiness*. Technical report edition. Cambridge: @Stake.

Tseng, Y, Ni, S and Shih, E. 2003. Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network. *IEEE Transactions on Computers*, 52(5):545–557.

Xylomenos, G. and Polyzos, G. 1999. TCP and UDP Performance over a wireless LAN. In: *Proceeedings of the IEEE INFOCOM.*

Xylomenos, G, Polyzos, G, Mahonen, P and Saaranen, M. 2001. TCP performance issues over wireless links. *IEEE Communications Magazine*, 39(4):52–58.

About the authors

Francois Mouton *is a PhD student at the University of Pretoria in the field of computer security and social engineering. He is also employed full-time by the CSIR to perform research on information warfare.*

Prof Hein Venter *is one of the founding members and current head of the Information and Computer Security Architectures (ICSA) Research Group in the University's Department of Computer Science.*