Improving Resilience against Node Capture Attacks in Wireless Sensor Networks using ICmetrics

Ruhma Tahir, Klaus McDonald-Maier
School of Computer Science and Electronic Engineering
University of Essex
Colchester, United Kingdom
rtahir@essex.ac.uk, kdm@essex.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have the potential of being employed in a variety of applications ranging from battlefield surveillance to everyday applications such as smart homes and patient monitoring. Security is a major challenge that all applications based on WSNs are facing nowadays. Firstly, due to the wireless nature of WSNs, and secondly due to their ability to operate in unattended environments makes them even more vulnerable to various sorts of attacks. Among these attacks is node capture attack in WSNs, whose threat severity can range from a single node being compromised in the network to the whole network being compromised as a result of that single node compromise. In this paper, we propose the use of ICMetric technology to provide resilience against node compromise in WSN. ICmetrics generates the security attributes of the sensor node based on measurable hardware and software characteristics of the integrated circuit. These properties of ICmetrics can help safeguard WSNs from various node capture attacks.**

Keywords-node capture attacks; ICMetrics; Wireless Sensor Networks; security

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of typically tiny nodes that are able to wirelessly communicate between themselves, and hence maintain communication without the need for human intervention [1]. These tiny low-cost wireless devices make wireless sensor networking a viable solution for a range of applications in WSNs [2]. However the wireless nature of WSNs also makes them susceptible to a range of passive and active attacks [3]; such as eavesdropping, routing attacks, node replication attacks, Denial of Service attacks and last but not the least the node capture attack, which has always been a major research challenge for researchers.

In a wireless sensor network, an attacker can compromise and gain access to the network as a legitimate user by capturing a sensor node in the network. This can generally mean extracting various attributes associated with the sensor node such as the cryptographic keys or even changing the hardware or software configurations associated with the sensor node.

Unless there is physical security [4] provided at the sensor node, they are vulnerable to node compromise attack, which can lead to the entire network being overtaken by attackers without even coming to know about adversarial presence in the wireless sensor network. But this is not a very practical solution, since making the sensor nodes tamper resistant results in an increase in the overall cost of the network. Therefore there is need to propose algorithmic solutions to the problem of node compromise in WSNs.

Cryptographic algorithms that are used to provide secure communication in WSNs depend on the use of stored encryption/decryption keys [5]. These algorithms have the inherent disadvantage that if a sensor node is compromised, it will lead to key/ secret information being revealed to the adversaries, which can ultimately result in even the entire network being overtaken and important data being revealed.

We propose the use of Integrated Circuit metrics or ICmetrics [6] as an alternative to stored encryption/decryption keys, for providing resilience against node capture attacks in WSNs. ICmetrics uses unique measurable properties and features of a hardware device to generate a basis number, which in turn can be used to generate the key. ICmetrics is very similar to biometrics where human properties and features are used to uniquely identify a person. The use of ICmetrics in WSNs removes the need for key storage; since the key is generated as and when needed based on the hardware/software characteristics of the sensor node. This feature safeguards WSNs from a node capture attack taking place on the network. Furthermore since the keys are generated every time, based on the designated hardware/software properties of the sensor node, any change to the hardware/ software configuration of the sensor node also never goes undetected.

The remainder of this paper is organized as follows; in section 2 we discuss the attacks inherent to WSNs since they are fundamentally different from traditional networks. In particular the node capture attack in wireless sensor network is discussed in section 3 which is the focus of this paper. To completely understand the possibility of a node capture attack taking place in any way, section 4 talks about its actual decomposition on passive attacks, active attacks and then a physical node capture taking place. Section 5 discusses the ICmetrics technology and its features. Section 6 elaborates on how ICmetrics is useful in safeguarding against node capture attacks in WSNs. To fully understand the threat model, section 7 outlines how ICmetrics will safeguard against node capture attacks by taking two

different scenarios of possible node capture attacks. The final section concludes our paper.

II. WIRELESS SENSOR NETWORK ATTACKS

Protecting sensor nodes in a wireless sensor network from attacks has been a major area of research since the advent of WSNs [7]. When we talk about security of hardware devices in general it is typical to think that protecting those devices means to protect them from unauthorized access and malicious software such as viruses; while physical security of the device is taken for granted.

However, the context in case of WSNs is much more complicated, particularly due to the broadcast nature of the wireless medium, which makes the network even more vulnerable to attacks; such as spoofing, altering and replaying of routing information, selective forwarding, sinkhole attacks, sybil attacks and wormhole attacks. Fig. 1 depicts a typical scenario of an attack that could possibly take place due to the wireless/ broadcast nature of WSNs. A wireless sensor network is composed of aggregator sensor nodes that gather and aggregate data from sensor nodes for selective forwarding, whereas sensor nodes typically sense their environment and forward data to aggregator nodes [8].

In WSNs due to the broadcast nature of the wireless medium, the data is broadcast to all the sensor nodes that lie within the range of any originating node, whether it is an aggregator node or simply a sensor node. Now as evident from Fig. 1, there is adversarial presence in the form of an intruder node in the network. Due to broadcast nature of communication taking place within the network, the intruder node will also receive the broadcasted data packets from all originating nodes if it lies in their communication range. This enables the intruder to gather information about the network to launch future attacks.

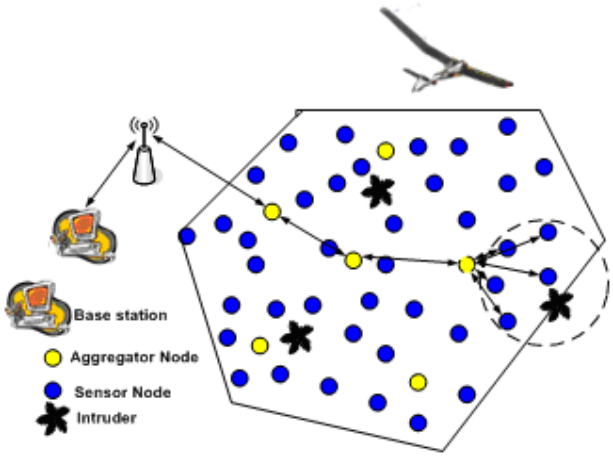

Figure 1. Wireless Sensor Network

Secondly their placement in hostile and unattended environments opens them to a range of attacks [9], which are particularly subject to their nature of not being physically protected as such. Since sensor nodes are accessible to the attackers, physical access control is not just as simple as denying access to the sensor node but there are much bigger issues there that need resolving.

Sensor nodes in WSNs are particularly vulnerable to attacks that aim to infect/ change hardware configuration and software characteristics of the data resident in the program memory. These types of attacks are usually referred to node capture attacks. Due to their severity of impact on the network, node capture attacks are one of the most pressing challenges in WSNs and to provide resilience against node capture attacks is a major issue [10].

III. NODE CAPTURE ATTACKS

Node capture attacks [11] enable attackers to capture the nodes in a WSN with having to do a lot of effort to launch the attack. The effect of node capture attack, as stated above can be to extract the cryptographic keys or manipulate the hardware/ software characteristics of the sensor node. Therefore, even if a single node is compromised, this can overtake the entire network. If node capture attacks are left undetected, they can have disastrous effects on the security of the network, since the whole network might have been overtaken without knowing it. This in effect may have an even bigger impact since it can lead to a larger class of attacks being launched on multiple networks. These attacks can result in complete loss of security within the network or even multiple communicating networks.

IV. THREAT MODEL

Node capture attacks are actually a hybrid of passive, active and physical attacks; these all work together for the actual node capture attack to take place. The aim of an adversary in a wireless sensor network is to gather as much information as possible about the network operation through passive and active participation, so as to successfully launch a node capture attack. From the attacker's perspective, the notion of a successful node capture attack is to gather as much information as possible about the network and then physically capture the node/s that lie at the heart of the whole network's operations and that can provide the attacker the maximum information to launch further attacks on maybe other networks.

WSNs work over wireless communication links so the nature of communication can easily aid the adversary in eavesdropping on the communication link. This also provides a chance for the adversary to silently capture important network information, either localized to a single node or all around the network.

If the data packets communicated throughout the network are encrypted, the adversary can extract important information from the packet headers which in turn can tell the attacker about the network structure, protocols being used and the network states. Once the attacker has gathered sufficient amount of information about the network, the attacker can start to actively participate in the network by

querying various nodes in different ways to gather as much information as possible or even sending malicious packets.

V. ICMETRICS-INTEGRATED CIRCUIT METRICS

ICmetrics or Integrated Circuit metrics makes use of system level characteristics to provide identification to the system [12]. It generates keys based on the hardware/ software characteristics and specification of the node. ICmetrics compute the required metrics on those hardware and software characteristics that are difficult for the attacker to deduce. These metrics/ features are not static but infact vary in a pre-determined fashion. For example, the address and value from the data transactions of a processor; its program address; and metrics for the effectiveness of the program and data caches derived from performance counters, etc [12].

After each key generation stage the produced encryption key is temporary and exists only locally, and the reproduction of the key once again takes place from measurable characteristics of the integrated circuit [14]. ICmetrics is not dependent on any particular encryption algorithm and there are no secret keys to share between the sender and receiver. ICmetrics generates an encryption key directly from measurable properties of a given hardware device, similar to the way biometrics extracts human features to perform an operation.

Analogous to biometrics, the features extracted from integrated circuits might not be stable, in that case the feature values may be based on values taken from a Gaussian distribution [13].

A. *Safeguarding against Node Capture Attacks using ICMetrics*

Traditionally to enable secure communication in a Wireless Sensor Network, encryption/ decryption has always been based on the use of stored keys for functioning of the network. However the use of stored keys to enable secure communication is threatened by the fact that, if the key used to encrypt the data is compromised, it will result in loss of data that is encrypted using the compromised key.

ICmetrics (Integrated Circuit metrics) will generate an encryption key based on certain unique and measurable hardware and software properties of the sensor node, which will greatly improve security, thus providing resilience to node capture attacks.

It makes use of hardware and software properties of the system thus providing resilience against tampering of hardware and software configuration. If tampering of these features takes place or if there is a change to the software executing on a particular hardware configuration, the generated private key forming as a result of recently generated ICmetrics will be different to the private key that was initially generated. This phenomenon in turn will prohibit the infected node from participating any further in the network operations, as will be evident from the node capture attack scenarios in the next section.

VI. NODE CAPTURE ATTACK SCENARIOS

In the following section we use two scenarios to further elaborate on the threat model of a node capture attack launched in WSNs.

A. *ICmetrics- Access to the Cryptographic Key*

In the first case of node capture attacks, once the adversary has gathered the required network information, the adversary's goal is to physically capture the sensor node and extract its cryptographic key associated with the node, so that it can decrypt all the information destined to the sensor node, as shown in Fig. 2.

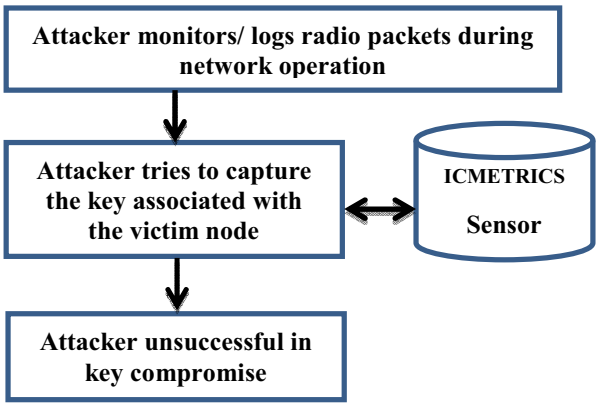

Figure 2. Threat model - key compromise

B. *ICmetrics-Manipulating the Hardware and Software Properties*

In the second scenario of node capture attacks, when the adversary is satisfied with the passive and active learning of information from the nodes/network, its goal is once again physically to capture the node and make changes to all the hardware and software configuration of the node. In this case of node capture attack, the attacker can make the sensor nodes work as and when needed rather than their normal operation. This process is further explained in Fig. 3 where the attacker's attempt to make changes to the system properties is unsuccessful.

ICmetrics has the ability to resist against this type of node capture attack, since any tampering with the hardware/ software properties of the sensor node will change its internal parameters, resulting in a different ICmetric being computed for the sensor node. This difference in the computed ICmetrics will cause an increase in the node's intra sample variance, and a decrease in the sensor node's inter-sample variance. This change will provide an indication that the sensor node has been tampered and the sensor node will not be able to take part in the network operation.

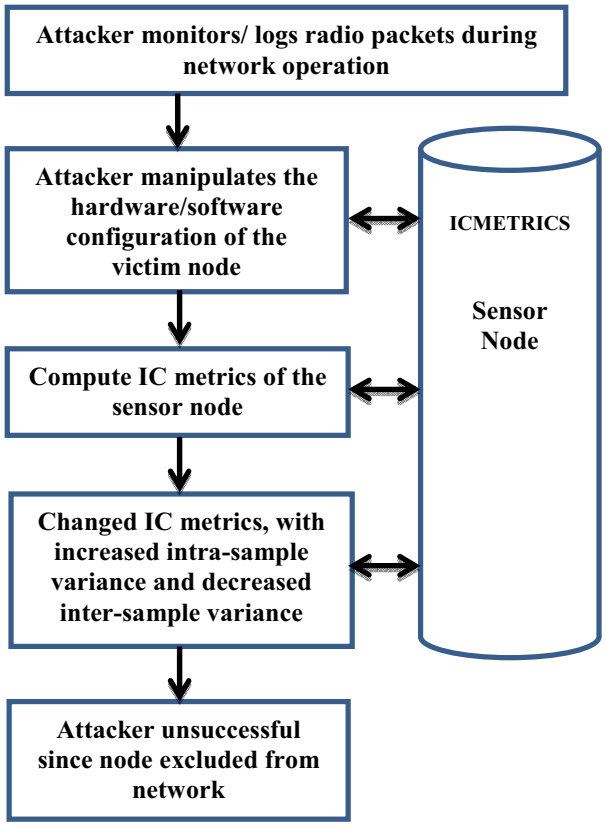

Figure 3. Threat Model – Manipulating Properties

VII. CONCLUSION

Wireless Sensor Networks are highly susceptible to node capture attacks due to the broadcast nature of the communication channel. Node capture attacks are a severe threat to the security of WSNs, since their threat severity can range from the compromise of a single node to the whole network being overtaken by an adversary. We propose the use of ICmetrics to safeguard WSNs against node capture attacks.

Very much like biometrics, the ICmetric technology computes the metrics based on the hardware/ software properties of the senor node, so it doesn't require a stored private key for the operation to take place. The key is computed as and when needed, safeguarding the node from compromise of the cryptographic key. Secondly any change in hardware/ software properties of the node generates a different ICmetric associated with the node, thus stopping it to take further part in the network. Therefore using ICmetrics, resilience against node capture is strengthened and overall survivability of the network is also enhanced.

VIII. FUTURE WORK

Our future plan is to test our scheme through experiments and analysis, thus benchmarking the results against existing schemes that provide security against node capture attacks. We expect that our proposed solution will be an efficient solution providing resilience against node capture attacks.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of the UK Engineering and Physical Sciences Research Council under grant EP/K004638/1.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, Vol.40, No. 8, Aug.2002, pp. 102-114.

[2] A. Perrig, R.Szewczyk, J. D.Tygar, V. Wen, and D.Culler, "SPINS: Security Protocols for Sensor Networks", Proc. 7th Annual International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy, July 2001, pp. 189-199.

[3] A. Perrig, J. Stankovic, D. Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, 2004, pp. 53-57.

[4] F. Armknecht, A. Hessler, J. Girao, A. Sarma, and D. Westhoff, "Security Solutions for Wireless Sensor Networks", Presentation, 17th Wireless World Reseach Forum, Heidelberg, Germany, Nov. 2006.

[5] E. Mykletun, J. Girao, and D. Westhoff "Public Key based Cryptoschemes for Data Concealment in Wireless Sensor Networks", IEEE International Conference on Communications, Istanbul, Turkey, June 2006, pp. 2288-2295.

[6] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Integrating Multi-Modal Circuit Features within an Efficient Encryption System", Third International Symposium on Information Assurance and Security, IEEE Computer Society Washington, DC, USA, 2007, pp. 83-88.

[7] C. Karlof, N. Sastry, D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 3-5 November 2004, pp. 162-175.

[8] Oly Mistry, Anil Gursel, Sandip Sen, "Comparing Trust Mechanisms for Monitoring Aggregator Nodes in Sensor Networks", Proceedings of the 8th International Conference on Autonomous Agents and Multiagent System, Richland, South Carolina, Vol 3, pp. 985-992.

[9] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of Sensor Network Protocols and Applications '03, Anchorage, AK, USA, 11 May 2003; pp. 113–127.

[10] A. K. Pathan, H. W. Lee, C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International Conference on Advanced Computing Technologies, 2006, pp. 1043-1045.

[11] P. Tague and R.Poovendran, "Modeling Adaptive Node Capture Attacks in Multi-hop Wireless Networks", AdHoc Networks, Vol. 5, No. 6, Aug. 2007, pp. 801-814.

[12] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Ensuring Secure Healthcare Communications via ICmetric based Encryption on unseen Devices", Symposium on Bio-inspired, Learning and Intelligent Systems for Security, Edinburgh, 20-21 Aug. 2009, pp. 113-117.

[13] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Integrating Feature Values for Key Generation in an ICmetric System," in IEEE NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2009) San Francisco, California, 2009, pp. 82-88.

[14] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Key Generation for Secure Inter-satellite Communication," in IEEE, NASA/ESA Conference on Adaptive hardware and Systems 2007, AHS-2007 Edinburgh, UK, 2007, pp. 671-681.