An Attack Tree Based Risk Assessment for Location Privacy in Wireless Sensor Networks

Conference Paper · September 2012

DOI: 10.1109/WiCOM.2012.6478402

3 authors, including:

Rong Jiang
National University of Defense Technology
15 PUBLICATIONS **705** CITATIONS
SEE PROFILE

Jun Luo
National University of Defense Technology
21 PUBLICATIONS **942** CITATIONS
SEE PROFILE

An Attack Tree based Risk Assessment for Location Privacy in Wireless Sensor Networks

Rong Jiang, Jun Luo, Xiaoping Wang
School of Computer
National University of Defense Technology
Changsha Hunan, China
{jiangrong, junluo, xiaopingwang}@nudt.edu.cn

***Abstract*—The challenging nature of insecure wireless channels and constrained resources make protection for wireless sensor networks (WSNs) an especially essential problem. The existing work has focused on preventive techniques to achieve location privacy protection, while the location privacy risk assessment receives less attention. In this paper, we propose a novel risk assessment approach to evaluate the risk of WSNs privacy based on attack tree. Using the attack tree model, we can estimate the degree that a certain threat might bring to the WSNs and identify possible attack sequences that an attacker may launch towards the privacy preserving system in WSNs. Then we adopted the multi-attribute utility theory to calculate the system's total risk value as well as the probabilities of each attack sequence. The analysis results can provide support for decision makers to make corresponding protection measures of location privacy.**

Keywords-wireless sensor networks; location privacy preservation; attack tree; risk assessment

I. INTRODUCTION

Nowadays the world has been scattered with smart devices offering tremendous convenience both to industry and final users. In such scenario, already known as the IOT-Internet Of Things, a lot of objects have been fitted up with computational and sensing capabilities[1, 2]. Wireless sensor networks (WSNs), which are ad hoc networks comprised of tiny resource-constrained sensor nodes, are basic component of the IOT. WSNs have been widely used in both military and civilian field such as battlefield surveillance, habitat monitoring, healthcare and traffic control [3]. However, due to the insecure wireless channels and constrained resources, WSNs are extremely vulnerable to various types of threats and attacks. Privacy preservation becomes extremely important especially when WSNs are deployed to monitor valuable asset or military targets, such as pandas or soldier movements. An adversary with the knowledge of the location of the data source or base station location may be able infer the content of the data being transmitted or destroy the monitoring objects.

Ozturk explored WSNs privacy issues first in [4] where the Panda-Hunter Game model was proposed and classified the privacy threats into content privacy and contextual privacy [5]. For the content privacy threat, the adversaries try to capture the packets in the networks to obtain the sensed data. Encryption technologies are used to counter this privacy threat. For the context privacy threat, the adversaries attempt to locate the position of some vital targets by eavesdropping the networks and traffic analysis techniques. Different schemes have been developed in the literature to counter such adversaries. The adversary model can be classified into local-adversary-based, group-adversary-based and global-adversary-based. The local-adversary-based schemes use weak adversary model assuming that the adversary can monitor only a small portion of the networks, typically similar to a normal sensor node's transmission range. Many techniques such as Probabilistic flooding [5], Phantom routing [5], Greedy random walking [6], and dynamical routing [7] have been proposed to counter such adversary. The group-based scheme assumes that the adversary distributes a group of monitoring devices in areas of interest to collect the traffic information in these areas. Mahmoud proposed a cloud-based scheme [8] for efficiently protecting source nodes' location privacy against such attack by creating a cloud with an irregular shape of fake traffic to counteract the inconsistency in the traffic pattern and camouflage the source node in the nodes forming the cloud. The global-adversary-based schemes assume that the adversaries are able to monitor all the traffic generated by the WSNs and therefore obtain the overview of the path followed by the messages. In order to deal with such powerful adversaries, the general solutions are to control the transmission rate [9], hide event messages with fake message transmissions [10] and dummy injection[11, 12]. However, the existing research on WSNs privacy preservation mainly focuses on the preventive techniques and fails to give a risk analysis from a system point of view for location privacy.

In this paper, we propose a novel risk assessment approach for location privacy preservation in WSNs based on the attack tree model. Attack tree method is used to model and analysis the risk of the system and identify the possible attacking strategies which the adversaries may launch. With the attack tree model, it is convenient to analyze the capability of the attack source and estimate the degree or the impact of a certain threat that might bring to the system. The multi-attribute utility theory is adopted to calculate the total probability of reaching attack goal. Then attack sequences are constructed to identify all the possible attacks to the location privacy in WSNs. According to the quantitative result, the decision maker of the system is able to find out which attacks are of the greatest possibility and decide what protection measures should be used to counter these attacks.

This work was supported by National Natural Science Foundation of China (61170261/F020809).

978-1-61284-683-5/12/$31.00 ©2012 IEEE

The remainder of this paper is organized as follows. In the next section, we introduce attack tree model and system model briefly and present how to build the attack tree. We assigned values to leaf nodes and calculated the system's risk in section III. In section IV, we carried out an analysis of attack sequences on the basis of attack tree. We conclude this paper and outline future works at last.

II. ATTACK TREE MODEL FOR WSNS LOCATION PRIVACY

A. Definition and Structure of Attack Tree

The attack tree approach, which provide a formal and methodical way of describing the security of systems based on varying attacks, was proposed by Bruce Schneier [13] to model threats against computer systems. A tree structure named attack tree is used represent attacks against a system, with the final desired goal as the root node and different ways of achieving that goal as child nodes. Each child node of the root becomes a sub-goal, and children of that node are ways to achieve that sub-goal. If one of those nodes cannot be divided further, it is a leaf node. Otherwise, those nodes are treated as sub-goals separately and are divided continually until all the events become leaf nodes. According to the logical relationship among them, those nodes, which are linked with an OR-gate or AND-gate, are OR nodes and AND nodes respectively. OR-gates are used to represent alternative attack methods and AND-gates are used to represent different steps toward achieving the same goal. The presentation of OR node and AND node is shown in Fig. 1.

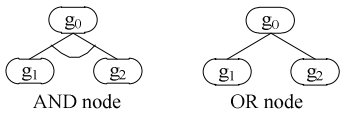


Figure 1. AND node and OR node.

B. Network Model and Assumption

We give a set of assumptions concerning the topology and shared security inherent in WSNs:

- The network contains a base station, which is significantly more powerful than the other nodes in the network. The base station, which is supposed to be secure and trusted, manages the networks and collects data from sensor nodes.
- We consider a typical sensor network comprised of a large number of resource-limited sensor nodes deployed in a field. The sensors are static and homogeneous. Each sensor node possesses an exclusive ID.
- Each node stores a cryptographic key IK shared with the base station and an initial one-way hash chain value ROF when it is deployed. The key IK is used for secret communication with the base station, and the ROF is used for verifying the legitimacy of messages broadcast by the base station.
- There isn't any tamperproof hardware in sensor nodes, thus if nodes are captured, their memory can be read or tampered with.

C. Attack Tree Construction

We perform a top-down, stepwise refinement strategy to construct the attack tree. Location privacy leakage, denoted by G, is set as the attacker's overall goal. The process of constructing the attack tree is as follows:

- Define the attacker's overall goal G: Location privacy leakage.
- Decompose the goal G into sub-goals: capture (M_1), eavesdropping (M_2), stealing (M_3) and purchase (M_4). The attacker's purpose can be achieved if any of the four components is reached. This list might be extensive and more sub-goals could be added.
- Continue the step-wise decomposition into smaller and smaller tasks. The completed diagram of attacks and sub-attacks is called an Attack Tree, as shown in Fig. 2.
- Assign attribute values to the leaf nodes. These values propagate up the tree. For attack probability, OR nodes have the value of their lowest child; AND nodes have the value of the sum of their children.
- Once attributes of all nodes are computed, one can calculate the security of the goal. If an attack costs the perpetrator more than the benefit, that attack will most likely not occur. However, if there are easy attacks that may result in benefit, then those need a defense.

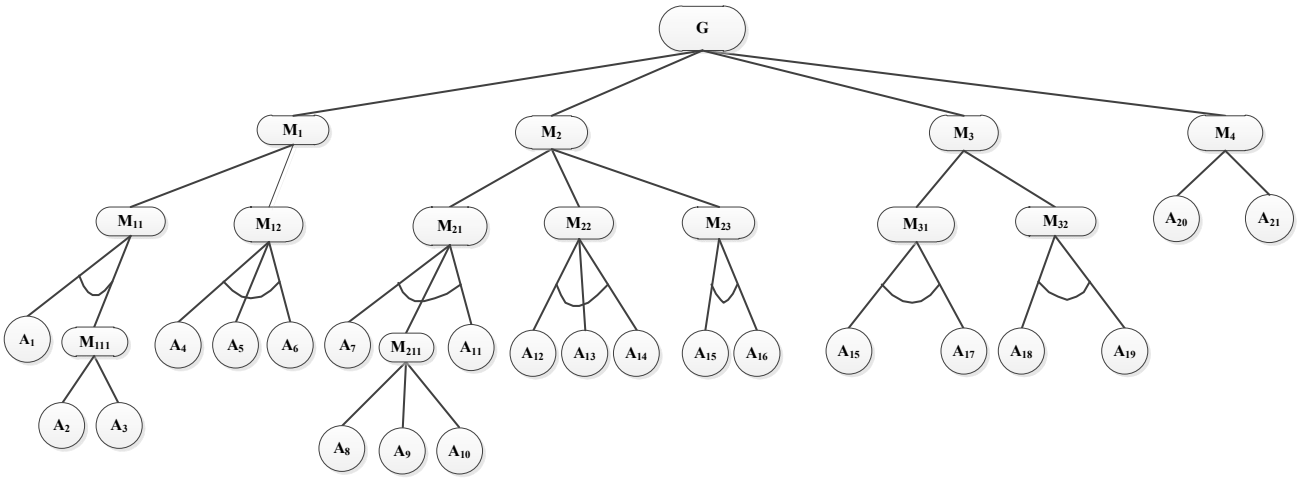
We take "capture (M_1)" and "eavesdropping (M_2)" in Fig. 2 for example to illustrate the attack tree construction, while the other sub-trees can be constructed in the same way.

There are two ways to achieve sub-goal "capture (M_1)".

- message leakage (M_{11}): Location information may be included in the messages. The attackers can learn about the location privacy by "obtain messages (A_1)" and "password cracking (M_{111})". The sub-goal M_{111} can be achieved by (A_2) or (A_3).
- node leakage (M_{12}): The attackers can carry out "look for node (A_4)", "crack node security mechanism (A_5)" and "search privacy information (A_6)" to get location information stored in the nodes.

In order to get a node's privacy by "eavesdropping (M_2)", as we have mentioned in section I, it is necessary to carry out:

- global eavesdropping (M_{21}): This mission can be achieved if three tasks are accomplished in a row: "deploy high-power monitor equipment (A_7)", "global traffic information collection (M_{211})" and "compute location privacy information (A_{11})". There are three ways to achieve M_{211}: "physical layer eavesdropping (A_8)", "MAC layer eavesdropping (A_9)" and "appliance layer eavesdropping (A_{10})".
- group eavesdropping (M_{22}): It can be launched through three joint atomic attacks: "deploy a group monitor equipment (A_{12})", "traffic information collection (A_{13})" and "analyze collected information (A_{14})".
- local eavesdropping (M_{23}): The attackers can "find the base station (A_{15})" and "follow the messages hop by hop (A_{16})" to locate the target.



G	leakage of location privacy	M_{111}	password cracking	A_{11}	compute location privacy infomation
M_1	capture	M_{211}	global traffic information collection	A_{12}	deploy a group monitor equipment
M_2	eavesdropping	A_1	obtain messages	A_{13}	traffic information collection
M_3	stealing	A_2	analytical reasoning	A_{14}	analyze collected information
M_4	purchase	A_3	Brute force attack	A_{15}	look for base station
M_{12}	message leakage	A_4	look for nodes	A_{16}	follow the messages hop by hop
M_{11}	nodes leakage	A_5	crack node security mechanism	A_{17}	crack system password
M_{21}	global eavesdropping	A_6	search privacy information	A_{18}	send malicious codes to base station
M_{22}	group eavesdropping	A_7	deploy high-power monitor equipment	A_{19}	malicious codes run in base station
M_{23}	local eavesdropping	A_8	physical layer eavesdropping	A_{20}	purchase from the third party
M_{31}	physical theft	A_9	MAC layer eavesdropping	A_{21}	leakage from the internal organization
M_{32}	malicious Code theft	A_{10}	appliance layer eavesdropping		

Figure 2. Attack tree for WSNs location privacy.

Note that, the attack tree described in Fig. 1 is only an example to capture the possible attacks launched by the attackers. As a general framework, an attack tree could accommodate more attack sub-tree by considering more attack strategies of the adversaries in practice. We believe that the recent research on the WSNs security and privacy preservation will also benefit the construction of the attack tree [1, 14].

TABLE I. GRADE STANDARD

Attack cost	Technical difficulty	Probability to be discovered	grade
>1	quite difficult	quite simple	5
0.8-1	difficult	simple	4
0.5-0.8	mediate	mediate	3
0.2-0.5	simple	difficult	2
<0.2	quite simple	quite difficult	1

III. RISK ASSESSMENT

The major challenge was to assign attribute values to attack tree nodes. There is no systematic method available to determine parameter values for each node in an attack tree. In order to evaluate these values, certain aspects of details of the system including protocol, hardware, application, operating system, environment as well as attack software and tool are needed. In this paper, we consider three attributes of the leaf nodes: attack cost c_A (which is the proportion of costs and benefits), technical difficulty d_A and the probability to be discovered s_A. The grade level standards are given in TABLE I. The assignment of each leaf's attribute requires knowledge of specific system. Since the main concern of this paper is on the new evaluation approach for WSNs location privacy, we attempt to assign values to the leaf nodes according to the following metrics and assigned values are shown in TABLE II:

- Powerful nodes, such as base station and cluster head, are capable of taking more protecting mechanism, so these nodes are more difficult to be compromised.
- The cost of radio monitoring equipment depends on their monitoring range. The global monitoring equipment is more expensive than the local one.
- An attacker could launch an attack on any layer of the system. The higher the attacked layer is, the more difficult for the attacker, and the lower the probability of success. In this condition, we can sort those layers according to the difficulty of compromise in the following order: application layer > transmission layer > routing layer > MAC layer > physical layer.

After value assignment for leaf nodes, these three attributes can be transferred into attackers' utility value P_A [15], which is the occurrence probability of a leaf node, according to multi-attribute utility theory. We applied the following formula (1) to calculate the utility of each leaf node [16]:

$$P_A = w_1 \cdot u_1(c_A) + w_2 \cdot u_2(d_A) + w_3 \cdot u_3(s_A) \qquad (1)$$

w_1, w_2 and w_3 are the utilities' correspondent weights, where $w_1 + w_2 + w_3=1$; Where $u_i(x)$ represents the utility function of the attribute, and their values fall into the interval of [0, 1]. Since all the three attributes are inversely proportional to their respective utility value, we suppose that the three utility functions $u_1(c_A)=u_2(d_A)= u_3(s_A)=u(x)=c/x$. Then we can calculate the occurrence probability P_A of each leaf node. We set $w_1+ w_2+ w_3=1/3$ and c=0.2 as an example and the occurrence probability P_A of each leaf node is shown in TABLE II. After that, we can obtain that the total probability of reaching the attack goal is 0.188 by transferring the attack tree into a BDD [17].

TABLE II. ATTRIBUTE VALUES OF LEAF NODES

leaf node	c_A	d_A	s_A	P_A	leaf node	c_A	d_A	s_A	P_A
A_1	1	2	3	0.122	A_{12}	3	2	1	0.122
A_2	4	5	3	0.052	A_{13}	3	2	1	0.122
A_3	3	2	4	0.072	A_{14}	2	1	2	0.133
A_4	2	2	3	0.089	A_{15}	1	2	2	0.133
A_5	3	5	3	0.058	A_{16}	3	5	3	0.058
A_6	2	4	2	0.083	A_{17}	3	4	4	0.056
A_7	4	1	1	0.15	A_{18}	1	3	4	0.106
A_8	2	2	2	0.1	A_{19}	3	2	4	0.072
A_9	3	3	2	0.078	A_{20}	4	2	5	0.063
A_{10}	3	4	2	0.072	A_{21}	3	2	1	0.122
A_{11}	3	4	1	0.106					

IV. ATTACK SEQUENCE ANALYSIS

On the basis of the attack tree, we can study the attacker's behavior by constructing attack sequences. An attack sequence S is a real path which an attacker can implement and is composed of a set of leaf nodes. The attacker can achieve the final goal in case that all the attack events of the nodes in the attack sequence occur. Once the attack sequences have been known, their probabilities can be worked out, and then we can compare them to figure out the attack sequence which the adversary may launch most likely. We can adopt Boolean algebra method to get all attack sequences of the attack tree. The probability of an attack sequence is the product of the probability of all the leaf nodes involved in the attack sequence. The attack sequences and their probabilities P_s are shown in TABLE III. From the TABLE III, we find that the attack sequence S_{11} may be the attack path most likely to happen. Thus, in order to keep location privacy in WSNs, it is necessary to pay more attention on it and adopt correspondent privacy preservation measures.

V. CONCLUSION

In this paper, we proposed a novel attack tree based risk assessment approach for location privacy in WSNs for the first time. We analyze the threats to the location privacy in WSNs from the system point of view and build an attack tree. We assign values to leaf nodes and adopt multi-attribute utility theory to calculate the system risk so that the assessment could be more objective. According to the attack tree model analysis, we point out and give some advice on improvement of location privacy in WSNs. In our future work, we will try to formalize the attack tree and build attack database for location privacy. With the help of the analysis, we will study location privacy preservation schemes with low energy consumption and delivery delay.

TABLE III. PROBABILITY OF ATTACK SEQUENCE

Attack Sequence	Leaf Nodes	P_S (10^{-2})	Attack Sequence	Leaf Nodes	P_S (10^{-2})
S_1	A_1, A_2	0.64	S_7	A_{12} , A_{13}, A_{14}	0.23
S_2	A_1, A_3	0.88	S_8	A_{15} , A_{16}	1.78
S_3	A_4 , A_5, A_6	0.04	S_9	A_{15} , A_{17}	0.77
S_4	A_7 , A_8, A_{11}	0.16	S_{10}	A_{18} , A_{19}	0.59
S_5	A_7 , A_9, A_{11}	0.08	S_{11}	A_{20}	7.22
S_6	A_7 , A_{10}, A_{11}	0.11	**S_{12}**	A_{21}	6.33

REFERENCES

[1] R. Rios, J. and Lopez, N, "Analysis of location privacy solutions in wireless sensor networks Privacy preservation in wireless sensor networks," Iet Communications, vol. 5, pp. 2518-2532, 2011.

[2] A. Bassi and G. Horn, "Internet of things in 2020-a roadmap for the future," Technical Report, Information Society and Media irectorategeneral of the European Commission and the European Technology Platform on Smart Systems Integration (EPSoSS), 2008.

[3] I. F. Akyildiz, W. L. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Ieee Communications Magazine, vol. 40, pp. 102-114, Aug 2002.

[4] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004, pp. 88-93.

[5] P. Kamat, Z. Yanyong, W. Trappe, and C. Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," in ICDCS 2005. Proceedings. 25th IEEE International Conference on, 2005, pp. 599-608.

[6] X. Yong, L. Schwiebert, and S. Weisong, "Preserving source location privacy in monitoring-based wireless sensor networks," in IPDPS 2006. 20th International, 2006, p. 8 pp.

[7] K. Pongaliur, L. Xiao, S. Min, Y. Yi, Z. Sencun, and C. Guohong, "Maintaining source privacy under eavesdropping and node compromise attacks," in Proc. of IEEE INFOCOM, Shanghai, 2011, pp. 51-55.

[8] M. M. E. A. Mahmoud and X. S. Shen, "A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot," IEEE Transactions on Parallel and Distributed Systems, in press.

[9] J. Deng, R. Han, and S. Mishra, "DecorrelatingWireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks," Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing System, vol. 2, pp. 159-186, 2006.

[10] Y. Jian, S. G. Chen, Z. Zhang, and L. Zhang, A Novel Scheme for Protecting Receiver's Location Privacy in Wireless Sensor Networks vol. 7, 2008.

[11] S. Min, Y. Yi, Z. Sencun, and C. Guohong, Towards Statistically Strong Source Anonymity for Sensor Networks, 2008.

[12] Y. Yang, M. Shao, S. Zhu, and et al, "Towards event source unobservability with minimum network traffic in sensor networks," in Proceedings of the first ACM conference on Wireless network security, Alexandria, VA, USA, 2008, pp. 77-88.

[13] S. B., "Attack trees," Dr. Dobb's Journal, vol. 24, pp. 21-29, 1999.

[14] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, Privacy preservation in wireless sensor networks: A state-of-the-art survey vol. 7, 2009.

[15] R. Sarin, Multi-attribute utility theory, Encyclopedia of Operations Research and Management Science 2001.

[16] D. D. Ren, S. G. Du, H. J. Zhu, and Ieee, A Novel Attack Tree Based Risk Assessment Approach for Location Privacy Preservation in the VANETs. New York: IEEE, 2011.

[17] Y. Sun, "A research on variable ordering methods of binary decision diagram," Shanghai JiaoTong University, Shanghai, 2008.