Computer Science and Information Systems 16(3):733–751 https://doi.org/10.2298/CSIS180918024C

A Novel SMP-based Survivability Evaluation Metric and Approach in Wireless Sensor Network

Hongsong Chen[1], Haiyan Zhuang[2], Zhiguang Shan[3], Chao-Hsien Lee[4], and Zhongchuan Fu[5]

[1] School of Computer & Communication Engineering, University of Science and Technology Beijing
Beijing 100083,China
chenhs@ustb.edu.cn
[2] Railway Police College
Zhengzhou, Henan, 450053, China
zhuanghaiyan@rpc.edu.cn
[3] State Information Center of China
Beijing 100045, China
shanzg@sic.gov.cn
[4] Department of Electronic Engineering, National Taipei University of Technology
Taipei City, China
chlee@ntut.edu.tw
[5] Department of computer science, Harbin Institute of Technology
Harbin 150001, China
15124585561@163.com

Abstract. In Industrial Internet of Things (IIoT) device and network, wireless sensor network (WSN) is an important component.Routing protocol is the critical component of WSN. As the WSN may be attacked by all kinds of intruders, the survivability of WSN is important to IIoT security. To precisely evaluate the systematic survivability ability under external attack and internal security mechanism,a novel survivability entropy-based quantitative evaluation metric is proposed to calculate the systematic survivability ability of WSN routing protocol. Numerical analysis and simulation experiments are combined to precisely calculate the survivability entropy metric.To validate the evaluation approach, NS2 (Network simulator) is used to simulate the DoS attack and security mechanism in WSN. Experimental results show that the novel survivability evaluation metric and method can precisely evaluate the systematic survivability ability of WSN.

Keywords: survivability entropy, quantitative evaluation, systematic survivability, wireless sensor network.

1. Introduction

With the rapid development of Industrial Internet of Things (IIoT), many smart devices are connected to Internet. With the convenience brought by the IoT and services, potential security problems and threats exist in the IIoT applications. In IIoT device and network, wireless sensor network is an important part of IIoT. Wireless Sensor Network (WSN) is applied in many aspects, such as industry automatic control, environment monitoring, smart home system. However, the security problems are hindering the wide application of WSN.

Routing protocol is the critical component of wireless sensor network (WSN). If the routing protocol is attacked, the survivability of WSN will be affected. As the attack behaviours are random, the consequences of attack are uncertain, it is difficult to quantitatively evaluate the change of survivability when the routing of WSN is attacked. There are some research progresses on the survivability of WSN, however, how to precisely evaluate the survivability of WSN routing protocol is a great challenge in current WSN security research area.

The generally definition of information system survivability was introduced by Ellison et al. [1]: Survivability is the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner. In the Federal Standard 1037C. [2], survivability is defined as the property of a system, subsystem,equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance. Although the definitions provide a good description of the concept of survivability, they do not provide mathematical precision to quantitative description of survivability. It is difficult to compare the survivability quantitatively by experimental method [3].

The remainder of this paper is organized as follows: in Section 2, related works and problem statement are analyzed. Survivability model for wireless sensor network routing protocol is described and derived in section 3. SMP-based Survivability evaluation method and novel metric are proposed in section 4. Simulation experiment and survivability precise evaluation are calculated in Section 5. The conclusions are made in Section 6.

2. Related Works and Problem Statement

2.1. Related Works

As the complexities of network systems, it is difficult to model and analyze the attacks for systematically analyzing network survivability ability. Xing Fei and Wang Wenye use semi-Markov process model to characterize the evolution procedure of node behaviors. The Semi-Markov-based node behavior model can be used as a bridge among some dynamic factors, such as node mobility or attack behaviour and network survivability [4]. They establish a survivability index system based on the Analytic Network Process (ANP) [5]. The ANP-based model of survivability index system was proposed to assess the survivability of Wireless Sensor Network in emergency communications.However, they do not provide experiment validation to the survivability model.

KIM Dong Seong etc have presented a survivability model framework for Wireless Sensor Network(WSN). The approach uses software rejuvenation to rejuvenate the sensor nodes under attack or/and compromised in a wireless sensor network [6]. They analyzed their model in mathematical manner and showed that software rejuvenation mechanism based on SMP and Discrete Time Markov Chain (DTMC) can decrease the failure probability while increases the probability of the system stayed in healthy state. Their model analysis is based on numerical analysis, the results can not reflect the real network scenario efficiently. Survivability model for cluster-based WSN was proposed, in which the state of each cluster is regarded as a stochastic process based on a Semi-Markov Process (SMP) and Discrete Time Markov Chain (DTMC) [7]. The isolation problem between clusters is researched and discussed. Quantitative survivability is calculated based on k connectivity metric. Numerical results show the model is effective. Experiment analysis should be considered to make the research results more effective.

Denial-of-Service and Black hole attacks are the two main problems in the security of ad hoc network. There are not satisfied solutions to solve the problems [8]. A novel multi-agent-based dynamic lifetime intrusion detection and response scheme are proposed to counter against the two types of attacks. Systematic impact and survivability metric should be considered in wireless network applications.The security of WSN and big data are the foundation of smart city [9]. Data security should be combined in the network security and survivability in smart city.

Attack tree based approach and stochastic model based approach are two main threat modeling method [10]. In tree modeling approach, the root node representing the attack goal and leaf nodes representing the ways of achieving the attack goal. Stochastic model based threat modeling approaches transform system state models to Markov chains and analyze them using finite state transition matrix or game theory. While experiment data should be filled into the model to make the method more effective.

A quantitative protection effectiveness evaluation method based on entropy theory is introduced [11]. They propose the protection intensity model, which can be used to compute the protection intensity of a stationary or moving object provided by a secure network. They presents a method for anomaly detection and classification based on Shannon, Rényi and Tsallis entropies of selected features, the construction of regions from entropy data using Mahalanobis distance [12]. They use One Class Support Vector Machine (OC-SVM) with different kernels (Radial Basis Function and Mahalanobis Kernel) for normal and abnormal traffic detection. Entropy is used to measure and analyze network traffic. Public transit network is a typical complex network with scale-free and small-world characteristics[13]. In order to analyze the survivability of public transit network, Fu Bai-Bai et al define new network structure entropy based on betweenness importance, the ”inflexion zone” is discovered which can be taken as the momentous indicator to determine the public transit network failure. The research object is about public transit network, the network survivability is dependent on the network structure parameters.

Dagdeviren O, Akram V K provides two localized distributed algorithms for determining the states of nodes. The first proposed algorithm identifies most of the critical and noncritical dominator nodes from two-hop local subgraph and connected dominating set information [17].

Xiue Gao and Keqiu Li propose a new method of evaluating the survivability of military heterogeneous networks, based on network structure entropy. A model of survivability is proposed based on the network irreversibility which considers not only the nodes but also the edges [18].

Security model in wireless sensor network and cloud computing are proposed and researched [19,20,21] They can be references to the security model in WSN.

2.2. Problem Statement

SMP and DTMC stochastic models can be used to build survivability evaluation model in wireless sensor network. Steady state probability and Mean Time To Security Failure (MTTST) are evaluation metrics of survivability model in stochastic process theory. Mean sojourn time and transition probabilities are the necessary parameters when calculating the steady state probability and MTTSF. In current research,as the attack behaviours are random and unpredictable, mean sojourn time and transition probabilities are computed by numerical analysis method. If we want to evaluate the survivability metrics precisely,experimental method should be used to obtain the mean sojourn time and transition probabilities in the survivability model.

However, the mean sojourn time and transition probabilities are difficult to be obtained by experimental method, thus steady state probability and MTTSF are difficult to be calculated precisely by traditional method. At the same time, traditional survivability metrics can not reflect the systematic changes caused by network attacks and security techniques. The changes of WSN routing protocol states will cause the change of network survivability ability. When the attackers intrude the routing protocol of wireless sensor network, how to precisely evaluate the attack effects to survivability ability of the WSN routing protocol is a great challenge. The research object is to propose a novel survivability evaluation experimental approach and metric in WSN routing protocol, the novel survivability evaluation approach and metric can reflect the dynamic characteristic under network attack and security mechanism.At the same time , the survivability metric can be measured by experimental method and calculated by mathematical formula.

3. Building the Survivability Model for Wireless Sensor Network Routing Protocol

3.1. Survivability Models in Wireless Sensor Network

Routing protocol is the key component of wireless sensor network, if the routing protocol is attacked, the wireless sensor network can not work normally, the survivability of the network will be affected greatly. The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead and determines unicast routes to destinations. Ad hoc On-Demand Multi-path Distance Vector (AOMDV) is the extended work of AODV routing [16]. AOMDV provide multipath to reach the destination, AOMDV is designed to solve the connectivity problem due to highly dynamic network topology. It provides multipath for data packets delivery from the source to the destination to mask the attack to route path. The routing protocols can be used to build routing paths of wireless sensor network. The survivability of AOMDV is higher than that of AODV because of the multi-paths characteristic of AOMDV routing protocol.

Survivability model should be built quantitatively and precisely to describe the change of survivability ability. Three types of survivability models are used to describe the survivability of wireless sensor network routing protocol. They are finite state machine model, DTMC model and SMP model. They are introduced in the following sections respectively. Dynamic transition behaviors of WSN routing protocol are described in finite state machine model. State transition probabilities are described in DTMC model. Steady-state probabilities and mean sojourn times are described in SMP model.

3.2. Finite State Machine(FSM)-based Survivability Model for Security AOMDV Routing Protocol

The routing protocol of wireless sensor network may suffer from all kinds of attacks, such as flooding attack, DoS (Denial of service) attack, Sybil attack, impersonation attack. The attacks will affect the survivability of routing protocol, multi-path routing and intrusion detection algorithm will be used to be against the attacks. So security AOMDV protocol will be in different states under different attack types and security techniques. Finite state machine model is used to describe the state transition process under different attacks and security schemes. The model is shown in figure 1.

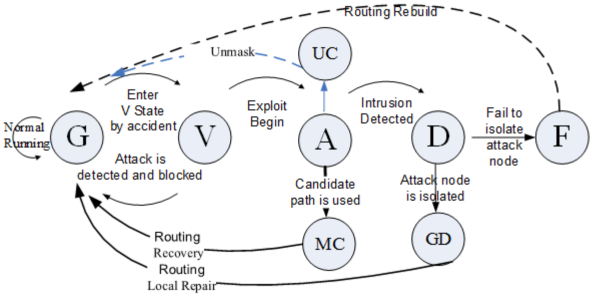

Fig. 1. FSM-based survivability model for security AOMDV routing protocol

As shown in figure 1, there are eight states in FSM-based survivability model of security AOMDV routing protocol. The state starts from good state to failed state, all the eight states come into being the whole life cycle of AOMDV routing protocol. They are listed in the table 1.

Table 1. Finite states and description

The name of state	Description of state
G	Good state
V	Vulnerable state
A	Attack state
MC	Masked compromised state
UC	Undetected compromised state
D	Detection state
GD	Graceful degradation state
F	Failed state

When AOMDV routing protocol runs normally, it is in Good state. When the attacker attempts to probe the network service and find the vulnerability, the system will enter the vulnerable state. If the probing behavior is detected and blocked, the system will be back to Good state. If the vulnerability is exploited by the attacker, the system will enter the attack state. As multi-paths can be provided by AOMDV routing protocol, if current routing path is attacked and the intrusion is in local scope, candidate path will be used to mask the attack. If the strength of attack is strong, the intrusion can be detected timely, the system will enter the detection state. When the intrusion can not be detected and masked efficiently, the system will enter the undetected compromised state. The system need to be reconfigured to recovery to good state. When the system enters into detection state, if the attack node can be isolated and controlled successfully, routing protocol can be back to good state; otherwise, the system will enter the failed state and signal an alarm, it needs rebuild routing to recovery to the good state. So the eight states reflect all possible conditions of AOMDV routing protocol under different attack and security techniques.

3.3. DTMC-based Survivability Model for Security AOMDV Routing Protocol

As the attack behaviors are random and the network topology is complex in WSN, the future state of system only depends on the current state, the state transition process has no relation to the past state, state transition process of the system meets the character of Markov process. As the state transition process of the system can be mapped to discrete time sequence, the transition of states can be represented by a serial of probabilities. The survivability model of system can be described by Discrete Time Markov Chain (DTMC). The DTMC-based survivability model for security AOMDC routing protocol is shown in figure 2,the system was given that the routing protocol was vulnerable, the DTMC model was consisted by a set of states and probabilities, only real lines are assigned to state transition probabilities because of multi possible states.

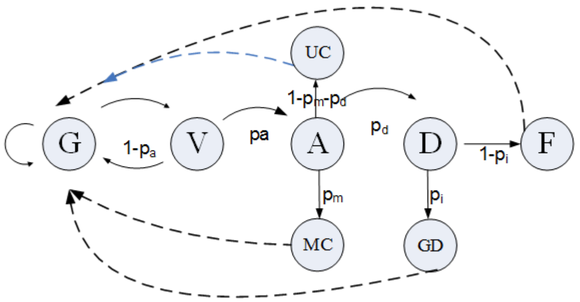

Fig. 2. DTMC-based survivability model for security AOMDV routing protocol

The state transition probability of DTMC model of security AOMDV routing protocol is shown in table 2.

The steady-state probabilities vector $\overline{v}$ of DTMC model can be computed as:

$$\overline{v} = \overline{v} \cdot P \tag{1}$$

Where $\overline{v}$= $[v_G, v_V, v_A, v_{MC}, v_{UC}, v_D, v_{GD}, v_F]$ and P is the DTMC state transition probability matrix, $\overline{v}$ stands for a eight dimensions row vector. The state transition probability

Table 2. Finite states and description

p_a	State transition probability from vulnerability state to attack state
p_m	State transition probability from attack state to Masked compromised state
p_d	State transition probability from attack state to detection state
$1 - p_m - p_d$	State transition probability from attack state to Undetected compromised state
p_i	State transition probability from detection state to grace degradation state
$1 - p_i$	State transition probability from detection state to failed state
p_a	State transition probability from vulnerability state to attack state
$1 - p_a$	State transition probability from vulnerability state to good state

matrix P describes the DTMC state transition probabilities between DTMC states which is shown in figure 2. The matrix P can be written as the formula2:

$$P = \begin{array}{c|cccccccc|} & G & V & A & MC & UC & D & GD & F \\ G & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ V & \widetilde{p}_a & 0 & p_a & 0 & 0 & 0 & 0 & 0 \\ A & 0 & 0 & 0 & p_m & \widetilde{p}_{md} & p_d & 0 & 0 \\ MC & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ UC & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ D & 0 & 0 & 0 & 0 & 0 & 0 & p_i & \widetilde{p}_i \\ GD & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ F & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} , \begin{cases} \widetilde{p}_a = 1 - p_a \\ \widetilde{p}_{md} = 1 - p_m - p_d \\ \widetilde{p}_i \ = 1 - p_i \end{cases} \tag{2}$$

Steady-state probability vector $\overline{v}$ should be satisfy with the constrain condition(3)

$$\sum_i v_i = 1, i \in \{G, V, A, MC, UC, D, GD, F\} \tag{3}$$

The DTMC steady-state probabilities can be theoretically deduced by equation 1,they are shown in formula 4.

$$\begin{aligned} & v_G = v_V(1 - P_A) + v_{MC} + v_{UC} + v_{GD} + v_F \\ & v_V = v_G \\ & v_A = v_V P_a \\ & v_{MC} = v_A P_m \\ & v_{UC} = v_A(1 - P_m - P_d) \\ & v_D = v_A P_d \\ & v_{GD} = v_D P_i \\ & v_F = v_D(1 - P_i) \end{aligned} \tag{4}$$

Conjunction with the equation 3 and equation 4,we can get the mathematical relationship between steady state probability and state transition probability, so steady-state probability v can be solved as formula 5:

$$\begin{aligned}
&v_G = \tfrac{1}{2+2P_a+P_aP_d} \\
&v_V = \tfrac{1}{2+2P_a+P_aP_d} \\
&v_A = \tfrac{P_a}{2+2P_a+P_aP_d} \\
&v_{MC} = \tfrac{P_m}{2+2P_a+P_aP_d} \\
&v_{UC} = \tfrac{P_a(1-P_m-P_d)}{2+2P_a+P_aP_d} \\
&v_D = \tfrac{P_aP_d}{2+2P_a+P_aP_d} \\
&v_{GD} = \tfrac{P_aP_dP_i}{2+2P_a+P_aP_d} \\
&v_F = v_D(1-P_i) = \tfrac{P_aP_d(1-P_i)}{2+2P_a+P_aP_d}
\end{aligned} \tag{5}$$

All steady-state probabilities of DTMC model can be solved by transition probabilities. So the steady state probability of DTMC can be calculated by the transition probability of system. If the value of v_G is greater, the value of v_F is less, the AOMDV routing protocol mostly runs in Good state, the survivability ability of AOMDV routing protocol is more powerful. Numerical analysis method is used to illustrate the relationship between steady-state probabilities and transition probabilities.To be numerical analysis method, the probability of detection and grace degradation can be set to 0.6. To solve the value of steady-state probabilities of DTMC model, transition probability values are set by expert experiences and related references[1,6,12]. They are given as the following:p_a=0.4;p_m= 0.3;p_d = 0.6;p_i = 0.6. By solving equations (4) and (5), steady-state probability values of DTMC model can be computed as: v_G=0.3289, v_V=0.3289, v_A=0.1316, v_{UC}=0.0132, v_{MC}=0.0395, v_D=0.0789, v_{GD}=0.0474, v_F=0.0316.

3.4. SMP-based Survivability Method for Security AOMDV Routing Protocol

A stochastic process is called a Semi-Markov Process if the embedded jump chain is a Markov chain, and the holding times (time between jumps) are random variables with any distribution. From the security researchers' viewpoint, the attacker's behavior and duration time are random, security response is diversified, vulnerability risk is uncertain, all these cause the sojourn time's distribution functions may be non-exponential. According to the definition of SMP(Semi-Markov Process), the survivability stochastic model needs to be formulated by SMP model. There are two types of parameters in SMP survivability model: mean sojourn time and steady-state probability in each state [14]. For computing the survivability measure, the steady-state probabilities $\{\pi_i, i \in X_s\}$of the SMP states should be computed firstly. Therefore π_i can be computed in terms of the embedded DTMC steady-state probabilities v_i and the mean sojourn times h_i [14]:

$$\begin{aligned}
&\pi_i = \tfrac{v_ih_i}{\sum_j v_jh_j} \qquad (i, j \in X_s) \\
&\textstyle\sum_i \pi_i = 1
\end{aligned} \tag{6}$$

Seen from the formula 6, π_i can be calculated by v_i and h_i , the sum of all steady-state probability π_i is 1, that is $\sum \pi_i = 1$. To calculate the the value of every π_i , $\sum_j v_jh_j$

should be calculated firstly, we use variable H to substitute the long mathematical express.From conjunction with the formula (5), we can get the mathematical express of $\sum_j v_j h_j$, which is shown as formula 7.

$$\begin{aligned}
&\textstyle\sum_j v_j h_j \\
&= \tfrac{h_G+h_V+p_\alpha h_A+p_{mc}h_{MC}+p_a(1-p_m-p_d)h_{UC}+p_a p_d h_D+p_a p_d p_i h_{GC}+p_a p_d(1-p_i)h_F}{2+2p_a+p_a p_d} \\
&= \tfrac{H}{2+2p_a+p_a p_d} = v_G H
\end{aligned} \tag{7}$$

Every steady π_i state probabilities can be calculated by equation 6 and 7, they are show in formula 8:

$$\begin{aligned}
\pi_G &= \frac{v_G h_G}{\sum_j v_j h_j} = \frac{v_G h_G}{v_G H} = \frac{h_G}{H} \\
\pi_V &= \frac{v_V h_V}{\sum_j v_j h_j} = \frac{v_G h_V}{v_G H} = \frac{h_V}{H} \\
\pi_A &= \frac{v_A h_A}{\sum_j v_j h_j} = \frac{v_G p_a h_A}{v_G H} = \frac{p_a h_A}{H} \\
\pi_{MC} &= \frac{v_{MC} h_{MC}}{\sum_j v_j h_j} = \frac{p_m v_G h_{MC}}{v_G H} = \frac{p_m h_{MC}}{H} \\
\pi_{UC} &= \frac{v_{UC} h_{UC}}{\sum_j v_j h_j} = \frac{p_a(1-p_m-p_d) v_G h_{UC}}{v_G H} = \frac{p_a(1-p_m-p_d) h_{UC}}{H} \\
\pi_D &= \frac{v_D h_D}{\sum_j v_j h_j} = \frac{p_a p_d v_G h_D}{v_G H} = \frac{p_a p_d h_D}{H} \\
\pi_{GD} &= \frac{v_{GD} h_{GD}}{\sum_j v_j h_j} = \frac{p_a p_d p_i v_G h_{GD}}{v_G H} = \frac{p_a p_d p_i h_{GD}}{H} \\
\pi_F &= \frac{v_F h_F}{\sum_j v_j h_j} = \frac{p_a p_d (1-p_i) v_G h_F}{v_G H} = \frac{p_a p_d (1-p_i) h_F}{H}
\end{aligned} \tag{8}$$

To obtain the sojourn time of every state, performance metric analysis method is used to analyze and acquire the sojourn time of every steady state.

4. SMP-based Survivability Evaluation Approach and Metric

In traditional survivability evaluation method [15], the steady-state availability of this system and Mean Time To Security Failure (MTTSF) are used to evaluate the survivability ability of system. While the evaluation metric can not reflect the whole system states' change and balance relation among different states. When attack occurs, the balance point among different states may be moved. How to measure the systematic change and balance point moving is a great scientific problem.

In information theory, entropy is a measure of the uncertainty associated with a random variable. The probability distribution of the events, coupled with the information amount of every event, forms a random variable whose expected value is the average amount of information. Entropy is calculated by the probability distribution. It is one of the evaluation functions for quantifying the diversity, uncertainty or randomness of a system. In wireless sensor network, the attack is random, the response to attack may be diversified, the routing protocol may stay in different state and keep different time. The systematic survivability of routing protocol in wireless sensor network is uncertain.We propose to use the information entropy method to quantitatively describe and explain the systematic change caused by external attack and internal security techniques. To describe the systematic survivability of wireless sensor network routing protocol, survivability entropy is proposed to quantitatively evaluate the systematic change and balance point moving condition.In information entropy theory, discrete information sources refer to that of discrete distribution on time and amplitude. The finite states in DTMC model and SMP model can be treated as discrete information sources. The steady state probabilities distribution of DTMC and SMP model can be treated as probabilities distribution of discrete information source.

As we know, the sum of discrete information source probability in information theory should be 1. As the sum of steady-state probabilities in DTMC and SMP model is 1, every state in SMP model can be treated as every discrete information source in Shannon information theory. According to the definition of information entropy, the steady-state probability distribution of SMP model can be treated as the probability distribution of distrete information source in information theory. According the definition of entropy, the mathematical formula of survivability entropy is shown as:

$$H(X) = E\left(\log \frac{1}{p\left(a_i\right)}\right) = -\sum_{1}^{n} p\left(a_i\right) \log p\left(a_i\right) \tag{9}$$

In the formula 9 , the number of states in SMP model is n, steady state probability of state i is $p\left(a_i\right)$. Seen from the formula 6, we know that $\sum_i \pi_i = 1$, they meet the condition of information source probability distribution in Shannon information theory. In SMP model, the survivability entropy can be expressAed as:

$$H(X) = E\left(\log \frac{1}{p\left(a_i\right)}\right) = -\sum_{1}^{n} p\left(a_i\right) \log p\left(a_i\right) = -\sum_{1}^{n} \pi_i \log \pi_i, i \in X_s \tag{10}$$

In formula 10, π_i stands for steady state probability of state i, X_s stands for the set of all possible states. $H(X)$ stands for system survivability entropy in SMP model. $H(X)$ reflects the average uncertain degree of system survivability in SMP model. Under attack or security conditions, attack or security conditions related state probabilities will change, at the same time, the sojourn time in related states will change, so the $H(X)$ will change with different attack or security conditions. We use condition entropy to express the change under condition y, it is shown in equation 11.

$$H(X|y) = E\left(\log \frac{1}{p\left(a_i|y\right)}\right) = -\sum_{1}^{n} p\left(a_i|y\right) \log p\left(a_i|y\right) \tag{11}$$

To describe the systematic change caused by the attack and security techniques, we use entropy difference to express the change quantitatively, it is shown in formula 12:

$$\varDelta H(X) = H(X) - H(X|y) \tag{12}$$

Entropy difference $DeltaH(X)$ is be used to quantitatively describe the systematic change caused by attack and security techniques. $DeltaH(X)$ can be used to express the systematic change by external attack and internal security technique, the entropy difference reflects the systematic changes and tradeoff between attack and security. Traditional performance metric can not describe the systematic change quantitatively.

5. Simulation Experiment and Survivability Evaluation

5.1. Simulation Experiment and Network Scenario

To precisely evaluate the survivability in wireless sensor network, we use simulation experiments to analyze and calculate the survivability entropy metric in SMP model. NS2 (network simulator 2) is a common software tool to do network simulation research. It is used to simulate the attack and record network simulation data. In SMP model, the survivability is related to mean sojourn time and steady-state probabilities in DTMC model. As the steady-state probabilities in DTMC model are calculated by the transition probabilities in DTMC, they are computed by numerical analysis method. The mean sojourn time can be obtained by simulation experiments in this paper. There are eight states in the SMP-based survivability model of wireless sensor network routing protocol. To recognize the eight states and compute the sojourn time, performance metrics analysis method are adopted.

If the attack is serious, the performance metrics will be changed significantly, the states can be recognized by the performance metrics, multi-metrics should be used to distinguish different states. Network performance metrics are used to detect the routing-level DoS attack and recognize the different states of SMP survivability model in wireless sensor network. Network Simulator 2 (NS2) is adopted to simulate the low-rate DoS attack behaviour, all the packets in network are recorded in the Trace file of NS2. Network performance metric and routing packets statistic can be obtained in the simulation trace file. Network scenario and attack model are described in the following, the network topology is shown in figure 3.

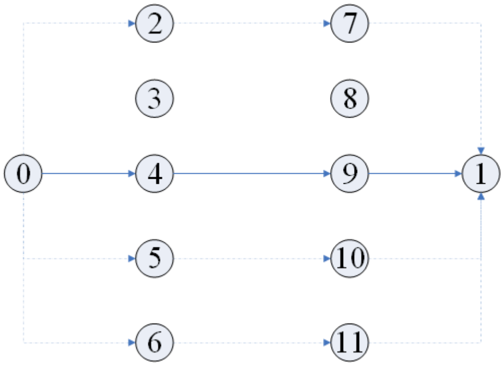

Fig. 3. Network simulation topology

The simulation configuration is shown in table 3,

Table 3. Network Simulation Configuration

Parameter type	value
Moving area	1000m * 1000m
Simulation time	200s
Number of nodes	12
Source node ID	0
Destination node ID	1
Attack node ID	5
Transmission protocol	TCP
Routing protocol	AOMDV
Application protocol	FTP
MAC layer protocol	IEEE 802.11
Attack type	Random RREQ flood attack
Attack duration	30-40s 60-100s
DoS Attack interval	0.03-0.08 s

To reflect the character of AOMDV multi-paths routing protocol, three different route paths are simulated in the simulation experiments; to embody the character of multi-hops routing protocol, there are three hops in the route path in the simulation scenario. So there are twelve nodes in wireless network simulation scenario in the paper,which is shown is figure 3. Node 0 is source node, node 1 is destination node, there are four routing paths between node 0 and node 1,they are 0-2-7-1,0-4-9-1,0-5-10-1 and 0-6-11-1.Node 5 is attack node. It sends a amount of Routing Request (RREQ) messages to other nodes to flood and attack the network connection. To simulate different flood attack severity, the number and interval of RREQ flooding packet are changeable in our experiments.

(1) Detection method

As the limited computing and storage resource of wireless sensor node, all network traffic is recorded in network trace file,performance metrics-based analysis method is used to detect the RREQ message flood attack. Reasonable performance metric thresholds are set to detect and block the attack. So routing protocol will enter different states under different attack strength and security mechanism.

(2) State recognize and separation

There are eight states in our survivability model. To recognize the different states in the model,three kind of performance metrics are used to separate the different states.They are packet loss ratio, network throughput, network delay. We use the three performance metrics to recognize the different states and calculate the sojourn time in every state.

(3) Mean Sojourn time calculation

Numerical analysis method can be used to analyze and calculate survivability parameters in traditional SMP model. However, numerical analysis method can not reflect the real attack and security status, so experimental method is used to calculate mean sojourn time of every state, numerical analysis method is used to compute the steady-state probabilities in SMP model. After all state in SMP model are recognized and separated in network simulation trace file, the sojourn time in every state can be easily calculated. Simulation experiment method is more accurate than traditional numerical analysis method.

5.2. State Separation by Performance Metric

NS2 can be used to simulate many network protocols over wired and wireless networks.It is used to simulate the AOMDV routing protocol and DoS attack in this paper. The following assumes that each state is recognized and separated by performance metrics and attack indicators, the metrics and indicators are deduced from simulation experiments and grade analysis. The goal of state separation by performance metrics is obtain the mean sojourn time, it is necessary parameter to the SMP model; the steady-state probabilities of SMP model are given by expert experiences and related references; so we use a hybrid approach to calculate the survivability ability of WSN routing protocol.

(1) State V

State V stands for vulnerability state,in which attacker try to do some probing and scanning,so network performances have been affected partially. Before DoS flood attack, the attack node try to inject some redundant route messages to network to probe the vulnerability of network routing protocol, so network performance can be affected locally. If the packet loss ratio has an increases less than 5%, the network throughput has a decreases less than 10%, and network delay has a increase less than 10%,the current state is considered to enter into state V.

(2) State A

State A stands for attack state, in which attacker has started a DoS attack to the routing protocol of wireless sensor network, so network performances have been affected significantly. If the packet loss ratio has an increases more than 5% and the network throughput has a decreases more than 10%,and network delay has an increase more than 10%, the current state is considered to enter into state A.

(3) State MC

State MC stands for mask compromised state, in which AOMDV routing protocol can mask some DoS attack by switching the attacked route path to a backup route path. By analyzing the network simulation trace file, the packet loss ratio increased more than 5%,at this time, routing path was switched to a backup path, that results in the packet loss ratio decreased near to normal value, the current state is considered to enter into state MC.

(4) State D

State D stands for detection state,in which the DoS attack can be detected by the intrusion detection algorithm. By analyzing the network simulation trace file, after the packet loss ratio increased more than 5%, routing path was not switched to a backup path, however,the indicator of intrusion detection is set to true, the attack nodes were detected,then the current state is considered to enter into state D.

(5) State UC

State UC stands for undetected compromised state, in which the DoS attack can not be masked and detected. By analyzing the network simulation trace file, after the packet loss ratio increased more than 5%, routing path was not switched to a backup path, the indicator of intrusion detection was set to false, the network throughput has a decreases more than 15%,and network delay has an increase more than 15%, the current state is considered to enter into state UC.

(6) State GD

State GD stands for graceful degradation state, in which the network system only maintains essential services, some wireless nodes are isolated to not join in the network. By analyzing the network simulation trace file, after the packet loss ratio has an increase more than 5%, routing path was not switched to a backup path, the indicator of intrusion detection is set to true, the attack nodes were detected and isolated to not to join in the wireless sensor network, then the packet loss ratio decreased to near normal value, the current state is considered to enter into state GD.

(7) State F

State F stands for failed state, in which the network system can not provide essential services,the DoS attack can not be controlled efficiently. If the packet loss ratio has an increases more than 10% and the network throughput has a decreases more than 20%,and network delay has an increase more than 20%, at the same time, no backup path can be used, the indicator of intrusion detection is set to true, however,the attack node can not be identified and isolated efficiently, the current state is considered to enter into state failed.The routing protocol need be recovered to normal state manually.

(8) State G

State G stands for good state, in which the network system works well,there are not any attack or probing behaviour in the network. All the network performance metrics and attack indicators show well.

So each state can be recognized by the performance indicators and related parameters, mean sojourn time can be calculated by the performance metrics and security indicators analysis from NS2 network simulation trace files.

5.3. Steady-state Probability and Survivability Precise Calculation

Numerical analysis method is used to show the relationship between steady-state probabilities and transition probabilities in DTMC model and SMP model. DoS (Denial of Service) attack is a kind of representative attack mode in wireless sensor network. We use DoS attack and intrusion detection technique to illustrate how to calculate the steady-state probability and survivability entropy in SMP model. As the DoS attack is a kind of representative attacks, according to the references [4,6,15] and our research experiences, the probability of detection P_d is set to 0.5,the probability of grace degradation P_i is set to 0.6, the probability from vulnerability to attack P_a is set to 0.4, the probability of masking attack is set to 0.3. According to the formula 5, steady-state probability in DTMC model can be calculated. They are calculated as the following: v_G=0.3333, v_V=0.3333, v_A=0.1333, v_{UC}=0.0267, v_{MC}=0.04, v_D=0.0667, v_{GD}=0.04, v_F=0.0267.

According to the formula 678, to solve the value of steady-state probabilities of SMP model, mean sojourn time should be calculated by the definition of every state.In our simulation experiment, the whole simulation time is 200s, the mean sojourn in Good state is set to 15s. Mean sojourn time can be acquired by simulation experiment and trace file analysis, then steady-state probability of SMP model can be calculated according to formula 6. As the intensity and interval of DoS flooding attack are changeable in some range, only some states appear in the experiments. We do three times of simulation experiments by NS2 and calculate the mean sojourn time of every state. The mean sojourn time is calculated,mean sojourn time h under different Attack Time Interval(ATI) are shown in table 4.

Table 4. Mean sojourn time h under different attack time interval

Mean sojourn time (s)	ATI=0.08	ATI=0.06	ATI=0.04	ATI=0.03
h_v	4.5	7.5	9	10.5
h_a	7.5	10	11	11.5
h_d	15	14	10.5	9.5
h_{gd}	20	14.5	15	10
h_g	1	15	15	15

Seen from the table 4, with the increase of DoS attack time interval, the mean sojourn time in vulnerability state to attack state are increased. Based on the mean sojourn time from simulation experiments, steady state probability of SMP model can be calculated by formula 6., they are listed in table 5.

Table 5. Steady state probability under different attack time interval

Mean sojourn time (s)	ATI=0.08	ATI=0.06	ATI=0.04	ATI=0.03
h_v	0.1613	0.2416	0.2786	0.3163
h_a	0.1075	0.1289	0.1362	0.1386
h_d	0.1075	0.0902	0.0650	0.0572
h_{gd}	0.0861	0.0561	0.0557	0.0361
h_g	0.5376	0.4832	0.4644	0.4518

At the same time, survivability Entropy (SE) under different attack time interval can be calculated by formula 10, they are listed in table 6.

Seen from the table 5, with the decrease of DoS attack interval,the strength of DoS flood attack increases. The steady state probability π_G, π_{GD} and π_D are decreased, while the steady state probability π_V and π_A are increased; the survivability entropy is increased firstly, then decreased. The experiment data shows that DoS attack can influence the network performance because of the different attack strength,thus the mean sojourn time of every state is affected, the WSN survivability will be changed as the change of every state. When the attack strength reaches some value, intrusion detection and multi-pathes masking will be triggered to improve the network performance and survivability, the attack is effectively suppressed by security mechanism,such as intrusion detection and muti-pathes

Table 6. Survivability Entropy under different attack time interval

SE	ATI
1.9021	0.08
1.9293	0.06
1.9077	0.04
1.8474	0.03

masking. Survivability entropy metric based on SMP model can reflect the survivability ability of the routing protocol in wireless sensor network, at the same time,the survivability entropy can reflect the dynamic change and trade-off between attack and security mechanism.However,traditional survivability evaluation metric can not reflect the systemic change

6. Comparison with Existing Methods

To explain the advantages of our approach, different items are used to compare our approach to existing methods,the comparison is shown in table7.

Table 7. Comparison our approach with existing methods

Comparison Items	Numerical calculus	Experimental calculus	Systemic survivability evaluation metric	computing complex
B. Madan[15]	support	none	None	medium
KIM et cl[6]	support	none	None	medium
Fei Xing et cl[4]	support	support	Network topology connectivity	high
Our approach	support	support	Network Survivability Entropy	medium

As shown in table 7, reference [6] and reference[15] only support the numerical parameter calculation, Mean Sojourn Time h dose not comes from experimental calculation,so the survivability calculus depends on the expert knowledge. Although the systemic survivability evaluation metric is supported in reference [4], the network topology connectivity information is difficult to be obtained in WSN environment, and the computing complex of survivability calculus depends on the connectivity probability problem of a geometric random graph, so the the computing complex in reference [4] is high.

However, Numerical Parameter calculus,Experimental Parameter calculus, systematic survivability evaluation metric are all supported in our approach, in addition to the analysis methods, a novel survivability evaluation metric-network survivability entropy is firstly proposed to describe the systematic survivability change of WSN routing protocol, at the same time, the computing complex of survivability calculus is medium, because our survivability calculus in formula 10 depends on the steady state probability of every state. Traditional surivivability evaluation approach is based on network topology structure, our approach is based on system-level states and changes. As the network topology structure is difficult to be obtained, our approach is more suitable to the WSN application environment. So our approach performs better than other existing methods.

7. Conclusion

Survivability evaluation is an important challenge in wireless sensor network security research.Because of the special characteristic of wireless sensor network,existing method is difficult to precisely calculate the survivability ability of routing protocol in wireless sensor network. A novel survivability entropy evaluation method is proposed to precisely calculate the survivability ability under DoS flood attack in wireless sensor network.

There are two main contributions in our research work:

1. Systematic survivability ability is firstly proposed and described by survivability entropy metric, which can describe the systematic survivability change of WSN routing protocol, it is validated by NS2 network simulation experiments.
2. Numerical analysis and simulation experiment methods are firstly combined to precisely calculate the survivability entropy metric,especially the sojourn time of every state was calculated by experiments. Experimental results show that the novel survivability entropy evaluation method is scientific and effective to precisely calculate the survivability ability of routing protocol in wireless sensor network.

Acknowledgments This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803403, Grant 2018YFB0803400, and Grant 2018YFB0505302, in part by the National Natural Science Foundation of China under Grant 61832012, in part by the National Social Science Fund of China under Grant 18BGJ071, and in part by the Fundamental Research Funds for the Central Universities under Grant TW201706.

References

1. R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survival Network Systems: An Emerging Discipline. Technical Report CMU/SEI-97-TR-013, SEI, CMU, http://www.cert.org/research/97tr013.pdf, 1997
2. Telecom Glossary 2000. Technical Report ANS T1.523-2001, Institute for Telecomm. Services, NTIA, DOC, http://www.atis.org/tg2k/, Feb. 2001,3
3. D. Chen, S. Garg, and K.S. Trivedi. Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks. Proc. ACM Int'l Workshop Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM '02), 2002: 61-68
4. Xing Fei, Wang Wenye. On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures. IEEE Transactions on Dependable & Secure Computing, 2010, 7(3):284-299
5. WANG Haitao, et al. Survivability evaluation index systems and evaluation models for Wireless Sensor Networks. IEEE 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD):2203-2207
6. KIM, Dong Seong, SHAZZAD, Khaja Mohammad, PARK, Jong Sou. A framework of survivability model for wireless sensor network. IEEE 2006 The First International Conference on Availability, Reliability and Security:514-522

7. C Chang, C Zhu, H Wang. Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attack. Internet of Things. 2012:126-132
8. Hongsong Chen, et al. Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol. Journal of Network and Computer Applications 30.1 (2007): 145-166
9. CHEN H S, HAN Z, DENG SN. Analysis and Research on Big Data Security in Smart City. Netinfo Security. 2015, (7):1-6
10. Goncalo Martins, Sajal Bhatia, Xenofon Koutsoukos, Keith Stouffer, Cheeyee Tang, Richard Candell. Towards a systematic threat modeling approach for cyber-physical systems. Resilience Week (RWS) 2015, 1-6
11. LV, Haitao, et al. Protection Intensity Evaluation for a Security System Based on Entropy Theory. Entropy, 2013, 15.7: 2766-2787
12. Azni A H, Ahmad R, Noh Z A M, et al. Systematic Review for Network Survivability Analysis in MANETS. Procedia - Social and Behavioral Sciences, 2015, 195: 1872-1881
13. Fu, Bai-Bai, et al. Survivability of public transit network based on network structure entropy. International Journal of Modern Physics C 26.09 (2015): 1550104
14. K. S. Trivedi. Probability and Statistics with Reliability, Queuing, and Computer Science Applications (2nd ed.). John Wiley & Sons, 2001
15. Bharat B. Madan, Katerina Goševa-Popstojanova, Kalyanaraman Vaidyanathan, Kishor S. Trivedi, A method for modeling and quantifying the security attributes of intrusion tolerant systems, Performance Evaluation. 2004,(56):167-186
16. Marina M K, Das S R. Ad hoc On-demand Multipath Distance Vector Routing. Network Protocols Ninth International Conference on ICNP. IEEE Xplore, 2001:14-23
17. Dagdeviren O, Akram V K, Tavli B. Design and Evaluation of Algorithms for Energy Efficient and Complete Determination of Critical Nodes for Wireless Sensor Network Reliability. IEEE Transactions on Reliability, 2018.
18. X. Gao, K. Li and B. Chen. Invulnerability Measure of a Military Heterogeneous Network Based on Network Structure Entropy. IEEE Access, 2018 (6):6700-6708
19. Aaron Zimba, Hongsong Chen, Zhaoshun Wang. Bayesian network based weighted APT attack paths modeling in cloud computing. Future Generation Computer Systems. 2019, 96(7):525-537
20. Hongsong Chen, Caixia Meng, Zhiguang Shan,Zhongchuan Fu and B. K. Bhargava. A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation. IEEE Access. 2019 vol. 7, pp. 32853-32866
21. Hongsong Chen, Ming Liu, Zhongchuan Fu. Using Improved Hilbert-Huang Transformation Method to Detect Routing-Layer Reduce of Quality Attack in Wireless Sensor Network. Wireless Personal Communications. 2019, 104(2): 595-615

Hongsong Chen (corresponding author) received the Ph.D. degree in Department of Computer Science from Harbin Institute of Technology, China, in 2006. He was a visiting scholar in Purdue University from 2013 to 2014. He is current a professor in Department of Computer Science,University of Science and Technology Beijing, China. His current research interests include wireless network security, attack and detection model, cloud computing security.

Haiyan Zhuang was born in May 1976, Female, Associate Professor of Railway Police College, Zhengzhou, China. Her research interested include information security, data analysis and mining, trust evaluation and computing.

Zhiguang Shan was born in 1974, PhD, professor and the director of Informatization and Industry Development Department, State Information Center of China. He also serves as the director of China Smarter City Development and Research Center. He received the B.A. degree in automation engineering, and the Ph.D. degree in computer science, both from the University of Science and Technology Beijing, Beijing, China, in 1997 and 2002, respectively. His main research interests include computer networks, performance evaluation, strategic planning and top design of smarter city, macro planning and developing policies of informatization. He has co-authored more than 70 papers in research journals and conference proceedings and 9 books in these areas.

Chao-Hsien Lee is Associate Professor,Department of Electronic Engineering, National Taipei University of Technology, Taipei City, Taiwan. His research area are mobile and information security, trust computing and Internet of Things.

Zhongchuan Fu received the Ph.D. degree in Department of Computer Science from Harbin Institute of Technology, China, in 2006. He is current an associate professor in Department of Computer Science,Harbin Institute of Technology. His research interested include computer system security, Fault tolerant computing, trust computing.

Received: September 18, 2018; Accepted: June 30, 2019.