Using Quantum-inspired Tabu Search Algorithm with Logic Operation and Moving Average Indicator for Wormhole Attack Detection in a WSN

Ting-Hui Chu, Shu-Yu Kuo, Yao-Hsin Chou

Department of Computer Science and Information Engineering, National Chi Nan University, Taiwan
{s100321905, s102321901, yhchou}@ncnu.edu.tw}

Abstract

Wireless Sensor Networks (WSNs) are composed of multiple sensor nodes which communicate with each other and one or more base stations wirelessly, and are applied in many fields, including military, ecological and environmental monitoring. However, the wormhole attack problem is a significant security issue in WSNs. The wormhole in the attack consists of one or more pairs of malicious nodes. They will receive and transmit the information of the neighbor node through a special tunnel to other wormhole nodes. This may result in many problems, such as packet routing errors, reduced node lifetimes and even damage the entire network topology. This paper improves a defense method that utilizes the neighbor information collected by mobile nodes without extra hardware, complex calculation or increased resource consumption. A moving average indicator combined with logic operation, the proposed method applies a Quantum-inspired Tabu Search (QTS) algorithm to effectively find combinations enabling the detection of wormholes. Finally, the experimental results show that the proposed method only uses the number of neighbors and can still effectively detect wormhole attacks.

Keywords: Wormhole attacks, Wireless sensor network, Quantum-inspired tabu search algorithm, Moving average, Logic operation

1 Introduction

Wireless Sensor Networks (WSN) are composed of a large number of sensors with small, low-cost, communication and computing power. WSNs have been widely applied in many fields, such as military, environmental and ecological monitoring. People deploy sensors in generally inaccessible or hazardous environments in order to collect data. Sensors communicate with each other by multi-hop transmission, sending their collected data back to base stations. However, such networks are vulnerable to malicious attacks like message eavesdropping [1] or modification, or the forgery of routes in the data transmission process. These attacks not only result in erroneous data routing but also reduce the lifetime of the involved sensors and compromise the overall network topology as the attacks result in additional power consumption [2-4]. This paper focuses on wormhole attacks, a type of WSN malicious attacks.

A wormhole consists of one or more pairs of malicious nodes, as shown in Figure 1. Regardless of the distance between the wormhole nodes, they can transmit information to each other by a special tunnel. When a node moves into the sensing range of the wormhole, the nearest wormhole node will collect that node's information, and transmit it to the other wormhole node/s through the special tunnel. This means that attacked nodes send packets through the attackers to the wrong route for faster delivery, and constantly retransmitting the message results in additional power consumption by the sensor node. As this means that the sensor node will have a much shorter lifespan than otherwise, this ultimately damages the entire network topology, such that data cannot be successfully transmitted back to the base station.

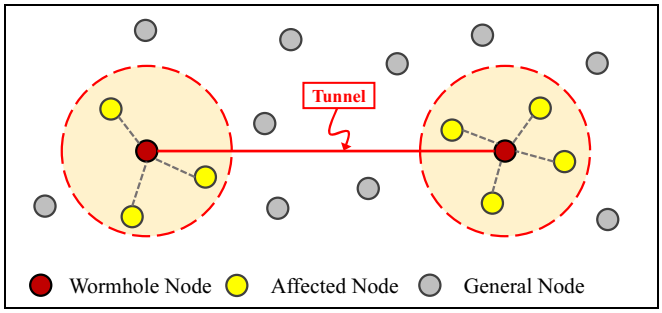

Figure 1. Wormhole attack

A variety of wormhole detection methods have been proposed, to date, to solve the wormhole attack problem. Some use directional antenna or Global Positioning System (GPS) to measure the intended

*Corresponding Author: Yao-Hsin Chou; E-mail: yhchou@ncnu.edu.tw
DOI: 10.3966/160792642019012001015

routing distance, thus identifying unusually located neighbor nodes. However, these special hardware devices are too expensive for low-cost sensors–and cost is a priority in the design of WSNs. Other methods require complex calculation, or significantly increased resources.

This paper offers an improved version; it does not require special hardware, and uses the number of neighbor nodes in the network, combined with logic operation and a Moving Average (MA), which is a common indicator in the financial field. This method can thus detect wormholes. The MA indicator utilizes the time series of price change to decide the strategy of a transaction. The developers of the method [3] viewed changes in the number of neighbor nodes just as economists would view price changes, and that such changes would provide a strategy for detecting wormholes. They also combined the logic operation and MA strategy to make the detection more accurate in order to avoid a single strategy causing a false positive. However, the combination of MA and logic operation cannot be exhausted in a short time. Thus, they used the Quantum-inspired Tabu Search (QTS) Algorithm to find the best wormhole detection rule in the vast solution space, combined with MA strategy and logic operation. Finally, this study improves the above method by including the characteristics of mobility model. As a result, the method is not only able to detect the presence of a wormhole for each node movement, but is also able to detect the movement of nodes into or out of a wormhole. The improved method uses fewer rules to detect the wormhole, while retaining good performance.

The remainder of this paper is arranged as follows: The different methods of wormhole detection are introduced in Section 2. Section 3 describes in detail how MA and logic operation are combined, and how QTS algorithm is used to find the best combination of MA and logic operation to detect wormholes. Section 4 presents the results and analysis of the experiment. Conclusions and the suggestions for future work are given in Section 5.

2 Related Works

2.1 Wormhole Detection

To date, many methods for detecting wormholes in WSNs have been proposed. Some use extra hardware to enhance detection ability or secure routing mechanisms against wormhole attack. Some observe the change in the number of neighbors. Some of these detection mechanisms are describe below.

Hu and Evans [4] proposed a countermeasure to prevent wormhole attack. Nodes use the directional antenna to send or receive a message at an angle to find a neighbor node that cannot come from this direction. That is, there are malicious nodes in this scenario. In [5-6], each sensor is equipped with Global Positioning System (GPS) to measure its position and calculate the path between any two nodes. If a packet is received from a node that is not within the sensing range, or the packet is received within an impossible arrival time, it indicates that a wormhole attack has occurred. However, GPS signal might encounter problems in some scenarios, such as in tunnels or areas covered by buildings; its efficacy may even depend on weather conditions.Packet leash [7] methods use two types of packet leashes, temporal leash and geographical leash. Temporal leashes, detect the wormhole by calculating the sending time and receiving time to find abnormal packet delivery times. However, the method requires an accurate time synchronization to calculate the packet delivery times, and the requirements will cause increased energy consumption. In geographical leash methods, the sender includes its own position and sending time, by which the receiver can estimate the maximum distance between them. However, the above methods also use additional hardware equipment, and these devices are too expensive for low-cost sensor networks.

Dong et al. [8] collected the location of all nodes in a network, and built the entire network topology. Assuming that the topology cannot be a flat graphic means the network is under wormhole attack. However, this method requires a lot of resources to collect information to maintain the topology, since the network topology is constantly changing. Song et al. [9] proposed a method called SWAN, in which statistical neighborhood information collected by mobile nodes. When a sensor moves into the transmission range of a wormhole node, the number of neighbors will be obviously increased. Once the number of neighbors is greater than a threshold, SWAN will observe this phenomenon as an indication of a wormhole attack. However, a fixed threshold in this method may result in misjudgment. In addition, the number of neighbors will decrease when a node moves to the boundary, and will return to the normal value after the node returns from the boundary. In these cases, the changes in the number of neighbors might also lead to misjudgment.

Shaon and Ferens [10] presented a scheme using an artificial neural network. This method detects wormhole attacks after collecting the number of neighbors. If the detector node moves into the wormhole-infected zone, the number of neighbors increases abnormally. The method must have sufficient information to determine the presence of a wormhole, however. The method proposed in this study, by contrast, is able to detect whether nodes are subject to wormhole attack with each node movement. Eidie et al. [11] used hello packets which set Time to Live (TTL) to 2 in order to obtain the 1-hop and 2-hop neighbors of each node in the network. If the 1-hop and 2-hop neighbors of a node increase dramatically, or by more than a threshold calculated by the number of neighbors

of all nodes, the node will be suspected as a wormhole. This method does not require extra hardware, but does require the cooperation of the neighbors of all nodes in the network. Chen et al. [12] presented a secure routing mechanism against wormhole attack which is based on the average distance per hop in the network. If the average distance per hop between two nodes is greater than the communication range, they concluded that a wormhole must be present. However, this method's errors increase as the distance between two wormhole nodes decreases.

This study improves a countermeasure [3] that also uses the change in number of neighbors to detect wormhole attacks without additional hardware devices, and in which each node can detect a wormhole without the cooperation of all other nodes. MA is calculated by the change of neighbors count, and is combined with logic operation to make detection more accurate. The QTS algorithm is then used to find the best combination of rules to detect wormholes in every step. However, the mobility model used in [3] is not very common, so this study exchanges it for a general one, and then uses the characteristic of the mobility model to propose a method that uses fewer resources, but still efficiently detects wormhole attacks.

2.2 Quantum-inspired Tabu Search (QTS)

QTS is a novel algorithm based on Tabu search and quantum computing. The primary characteristic of the algorithm is that the uncertainty before measurement increases the possibility of generating different solutions. The quantum states are then updated using better and worse solutions. QTS can be guided towards better solutions and away from worse solutions in order to effectively explore the solution space. QTS can also be applied in different optimization problems with outstanding performance results, such as the 0/1 knapsack problem [13], synthesizing optimal reversible circuits [14], Function Optimization [15] and combination of trading rules [16-19]. In these problems, it is inefficient to exhaust all solutions of these problems because the process may be very time-consuming. The QTS algorithm is thus to find the better solution faster. In the wormhole detection problem, QTS is used to find the best combination of MA rules in less time in order to effectively detect wormhole attacks, with outstanding performance results.

3 Proposed Scheme

The previous Section described some detection mechanisms. They use special hardware, time or distance analysis to detect wormhole attacks. However, the proposed method does not require special hardware devices and complex calculation, and uses only the number of neighbors, which is usually collected. This section describes how logic operation and Moving Average (MA) are combined in the proposed method. Quantum-inspired Tabu Search (QTS) algorithm is then used to find the best combination of rules. In the scenario used, each sensor has the same transmission range, as do the wormhole nodes. Therefore, the first node is selected as the observation node to detect wormholes. The following divides the proposed method into five steps, and describes them in detail.

3.1 Mobility Model

This study uses the Random Waypoint Model (RWP) 20-21] as the basis for node movement. Each node moves independently of other nodes, but all nodes have the same stochastic movement properties.Initially, nodes each have their own position, destination, velocity and pause time. Figure 2 illustrates the mobility model of nodes. The node moves toward the destination with fixed velocity, and calculates the number of its neighbors in every movement. A node will select the next destination and velocity in the scenario when it arrives at its destination.

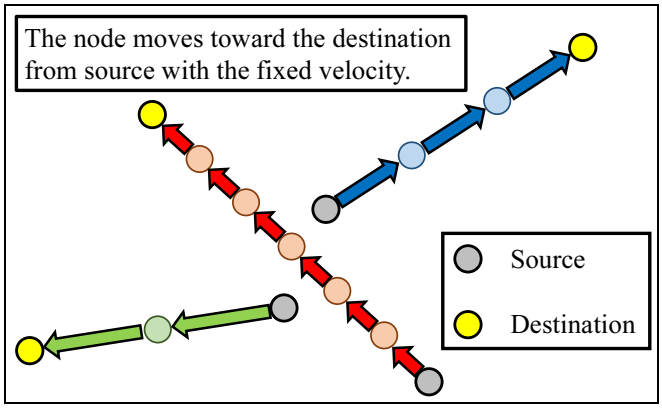

Figure 2. Random Waypoint Model

A node chooses a new velocity V uniformly at random from the interval $[v_{min}, v_{max}]$. This study requests that $v_{min} > 0$ in order to prevent nodes remaining in a static state in the movement process. In this paper, the velocity is set at between 1 m⁄s and 20 m⁄s. The node is continuously attacked by a wormhole when it moves at slow velocity into the transmission ranges of wormhole nodes, or moves through the edge of the affected zone of a wormhole, as shown in Figure 3. Since the initial position and destination of each node are uniformly distributed in the scenario, there will be no confusion as to whether the node should go through or bounce off the boundary.

3.2 Adversary Model

This paper assumes a pair of wormhole nodes in its scenario. Unlike general nodes, wormhole nodes posit in a fixed location and attack neighboring nodes. Wormhole nodes then send the information of those neighboring nodes to other wormhole nodes, and then

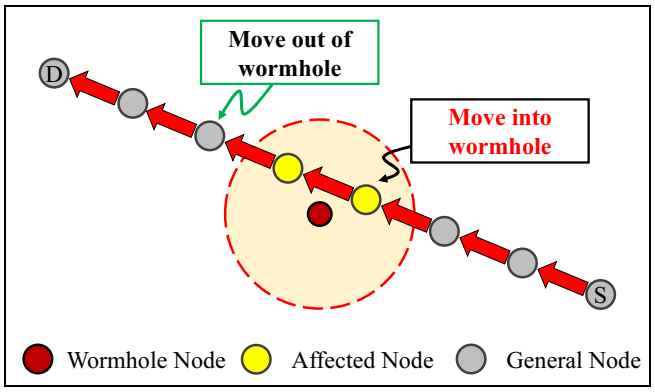

Figure 3. Node continuously attacked by a wormhole

the neighboring nodes of those other wormhole nodes by the special tunnel between the two wormholes nodes. This misleads the attacked nodes into transmitting data along the wrong route. Furthermore, the situation in which there are no neighbors near a wormhole node, as such a wormhole attack would have no effect on the number of neighbors.

3.3 Combination of MA and Logical Operation

The Moving Average(MA) is a common technical indicator used to predict future data by analysis time series data in the financial field. This study uses SMA, which means the weight of the daily price of stock is the same; that is, the arithmetic average of the price of stock in a period of time. Calculating the different periods of MA reflects the changes in price of stock and trends. When a short-term MA crosses above a long-term MA, it is called a golden cross, while a death cross is the converse. In this study, the change in the number of neighbors per movement in a WSN is considered as similar to daily changes in stock prices, If MA is applied to detect wormhole attacks, it may be taken as a signal of a wormhole attack. This phenomenon can also be viewed as a signal that a node has moved into or out of the transmission range of a wormhole. This study replaces the number of days and the stock price values with the number of movements and the number of neighbors of a node, and the MA formula is as follows:

$$MA = \frac{n_p + n_{p-1} + \cdots + n_{p-(m-1)}}{m} \quad (1)$$

where n_p is the present neighbors of a node, and m is the number of movements. The common time periods are days, weeks, fortnights, months, seasons, half-years and years, respectively, or periods of 1, 5, 10, 20, 60, 120 or 240 days. This study expands the seven time periods to the period from 1 to 256, so that the choice of strategies to detect wormholes becomes more diversified. MA is calculated by the number of neighbors during the movements of a node. However, the authors believe that the MA strategy can be used to detect wormhole attacks. For example, MA(20,120) represents that MA(20) crosses above MA(120); that is, the node is being attacked by a wormhole, as shown in Figure 4.

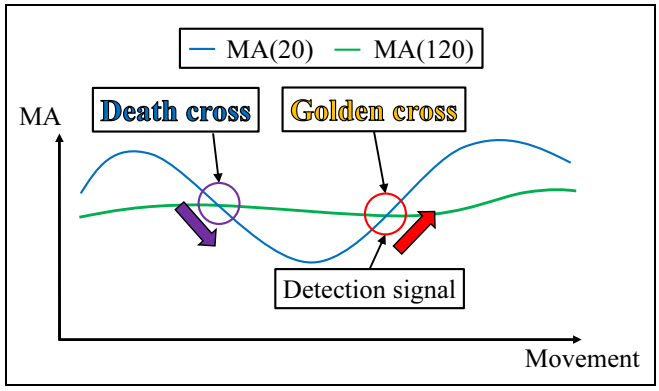

Figure 4. Example of MA(20,120) cross

The above explains how MA can be applied to detect wormhole attacks, calculating the number of neighbors to detect wormholes. However, using only one strategy is unreliable. The number of neighbors will decrease when a node moves to the boundary, and will increase if a node returns from the boundary. False positives may also occur if a node simply has very few neighbors: this could be mistaken for the node moving into a wormhole.

Likewise, if a node has very many neighbors, it could be mistakenly identified as moving out of a wormhole. Therefore, logic operation was combined with the MA strategy. Logic operation consists of AND and OR logic gates. Combining multiple strategies with AND gates yields a rule, such as MA(1,50) $\wedge$ MA(3,94). When two strategies' signals cross at the same time, it indicates that the node has been attacked by a wormhole. However, it is still risky to judge each wormhole attack by one rule, so this study combined multiple rules with OR gates to a rule base, which can detect different wormhole situations, as Figure 5 shows. If a signal appears from [MA(3,60) $\wedge$ MA(120,94)] or [MA(7,125) $\wedge$ MA(76,88)], it is judged that the node has been attacked by a wormhole.

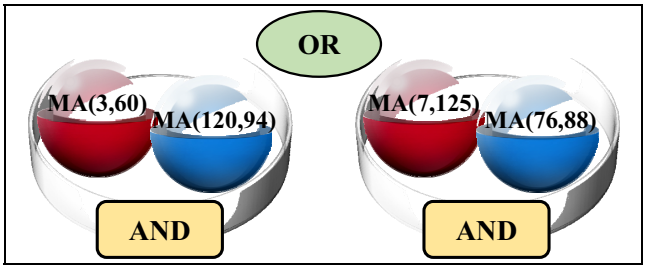

Figure 5. Combinations of rules

Because using only one wormhole detection strategy will cause some misjudgment, this study thus uses AND gates. It also uses multiple rules, combined by OR gates, to detect wormhole attacks from different movements, which improves the detection accuracy.

3.4 Detection Accuracy

Hypothesis testing is a common tool in statistics. Null hypothesis is used when a researcher wants to know the accuracy of target, and the alternative hypothesis is used to refute the null hypothesis. In this paper, the null hypothesis H_0 is that with wormhole attack at present; otherwise, the alternative hypothesis H_1 without a wormhole attack. It means that it is assumed that a wormhole attack is taken place until there are proven otherwise. There are four possible outcomes of this method, as shown in Table 1.

Table 1. The confusion matrix

Total population	Condition positive (H_0)	Condition negative (H_1)
Prediction positive	True Positive (TP)	False Negative (FP) Type I error
Prediction negative	False Positive (FN) Type II error	True Negative (TN)

The quality of the rule bases is evaluated by detection rate. The detection rate D_W with weight was proposed in [22], and the weight is based on the ratio of the sensing range of the wormhole to the size of the scenario. This study uses a more intuitive detection rate D, which is calculated as the number of successful judgments divided by the total number of judgments, and this is calculated for each movement. The formula is as follows:

$$D = \frac{N_{\text{successful\_judgment}}}{N_{\text{total\_judgment}}} \quad \textbf{(2)}$$

Successful judgments are divided into two cases, true positives (TP) and true negatives (TN), which are situations in which an attack is detected, and the node is actually not attacked or attacked by a wormhole, respectively. Total judgment is divided into four cases, namely true positive (TP), true negative (TN), false positive (FP) and false negative (FN).

3.5 QTS Algorithm

The above describes the combination of MA and logic operation to detect wormhole attacks. The total number of combinations of rules is 256^4, equivalent to more than 4.2 billion combinations if the MA period is expanded from 1 to 256 and combined with one AND gate. Therefore, QTS is used to find the best combination of rules for detecting when a node moves into or out of a wormhole. The detailed description of QTS and its flow chart is as follows:

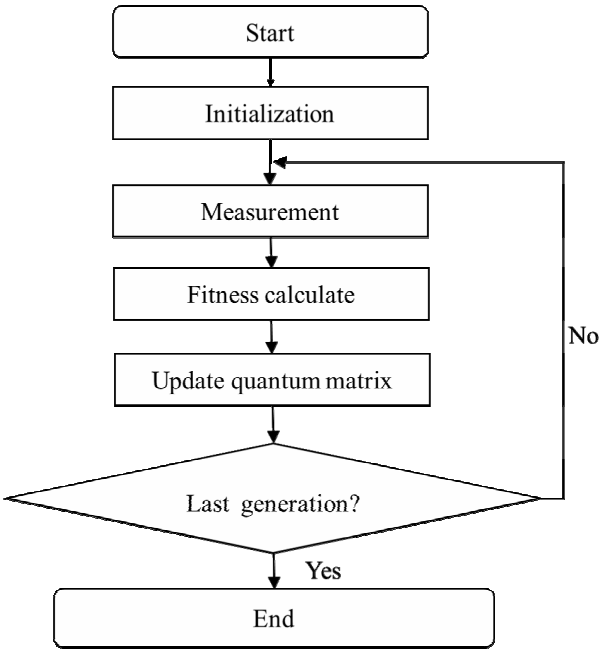

Figure 6. The flowchart of QTS

3.5.1 Initialization

In the first step, a quantum matrix is initialized. Quantum characteristics are simulated, specifically that quantum bits have a 50% chance of being 0 or 1 before being measured. The quantum matrix is then initialized with a value of 0.5. The proposed method uses binary encoding and expands the MA period. So 8 qubits are required, encoded as 2^0 to 2^7, representing the MA period 1~256. For instance, an MA strategy requires $8 \times 2 = 16$ qubits. If one AND gate is used to combine the two strategies, then $16 \times 2 = 32$ qubits would be required to initialize a quantum matrix, as follows:

$$Q_m = [0.5, 0.5, 0.5, ..., 0.5] \quad \textbf{(3)}$$

3.5.2 Measurement

In this step, S solutions, which have the same number of bits as the quantum matrix, are measured to produce the MA rules. A random variable R from the interval [0,1) is used, and R is compared with each qubit in the quantum matrix. If R is less than a qubit, the bit in the solution is set to 1; otherwise, it will be set to 0, as in Table 2.

Table 2. Example of producing solutions

Produce solutions			
Number of qubit	1	2	3
Quantum matrix	0.5	0.5	0.5
Random Variable R	0.69	0.42	0.88
Solution	0	1	0

The 32 bits of the solution are then transferred to a rule combining two strategies with one AND gate, as shown in Figure 7.

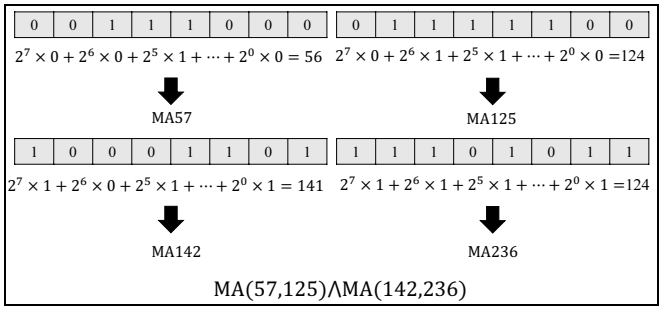

Figure 7. Combining two strategies with one AND gate

3.5.3 Evaluating the Fitness Function

After solutions are produced, their fitness can be calculated. In order to detect when the node moves into or out of a wormhole, QTS is used to find two rules, respectively. So, the fitness of solution is the number of successful judgments that a node has actually moved into a wormhole. On the other hand, the other solution fitness is the number of successful judgments that a node has actually moved out of a wormhole. Whether the judgment is correct or not will affect the performance of the detection rate.

3.5.4 Update Quantum Matrix

In this step, it is expected that the obtained solution will be nearer the best solution, and farther from the worst solution. Thus, the global best solution is found, as is the worst solution, from S solutions. The bits of the two solutions are then compared. If the two bits are different, the qubits of the quantum matrix are adjusted with θ, with a value of 0.008 0, as in Table 3. After the quantum matrix is updated, the probability of measuring better rules in next generation is higher.

Table 3. Example of update quantum matrix

Solutions and Quantum matrix					
Number of qubit	1	2	3	4	5
Best solution	0	1	1	0	1
Worst solution	0	0	1	1	0
Quantum matrix	0.5	0.5	0.5	0.5	0.5
Updated matrix	0.5	0.508	0.5	0.492	0.508

QTS is used to find a rule that can detect a few situations where the node moves into or out of a wormhole. Then, QTS is used repeatedly used to find other rules, and combine multiple rules for a rule base with an OR gate until two rule bases can respectively detect all situations where the node moves into or out of a wormhole. Finally, the two rule bases are used to detect wormholes. If two signals are produced by the two rule bases respectively, then the node has been attacked by a wormhole between these two signals. The following section shows the results of the simulation experiment.

4 Simulations

This section analyzes the results of experiments conducted, and compares them with those obtained using other methods. It also describes the parameters used and simulation scenario.

4.1 Simulation Environment

The simulation is implemented using C#, and the parameters for the environment and the Quantum-inspired Tabu Search (QTS) algorithm settings are given in Table 4 and Table 5. In the simulation setup, 100 sensor nodes are distributed in a square 500 m by 500 m area. Random Waypoint Model (RWP) is used as the mobility model for the simulation. Each node moves 500 steps in each map. A pair of wormholes is placed on the locations at 150 m by 150 m, and 350 m by 350 m. Every node has a transmission range of 50 meters.

Table 4. Environmental parameters

Scene area	500*500 m^2
Number of nodes	100
Transmission range	50meters
Location of wormholes	(150,150),(350,350)
Number of maps	30
Number of movements in each map	500

Table 5. QTS parameters

Number of solutions S (populations)	300
Number of generations	300
θ	0.008

For the QTS parameters, 300 populations and 1000 generations were used. The value of θ, by which the quantum matrix is adjusted, is 0.008 0.

4.2 Simulation Result and Analysis

4.2.1 Experiment Analysis of Proposed Method

In proposed method, the max Moving Average (MA) period is expanded to 256, and MA strategy is combined with logic operation. The solution space is 256^4 if 1 AND gate is used. More AND gates will increase the solution space exponentially, and it will become more difficult for the rules to produce signals simultaneously. However, the rules must be found in a sufficiently timely manner to effectively detect wormholes. Therefore, it becomes necessary to know how many AND gates are suitable for QTS. First, the average detection accuracy results of 1000 experiments with different numbers of AND gates are compared.

100 nodes are used, and their transmission range is 50 m. As in Figure 8, 1 AND gate produces an 87.98% detection accuracy, which is better than other results. The average number of successful detections when the node moves into or out of the wormhole in 1000 experiments is compared for different numbers of AND gates.

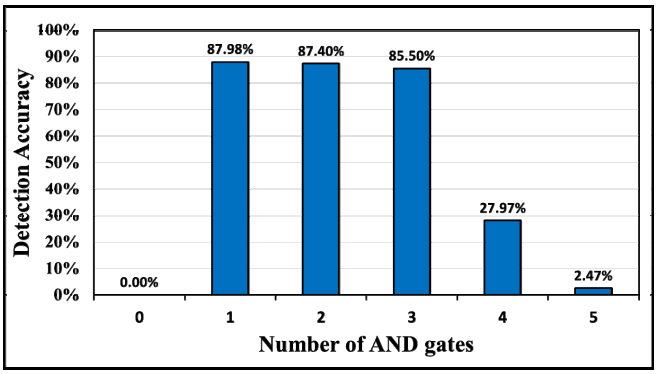

Figure 8. Comparison of numbers of AND gates

As in Figure 9, there is no successful detection when no AND gate is used (only one detection strategy employed). Using 3 or more AND gates reduces successful detections. Both 1 and 2 AND gates have great performance. However, the use of 2 AND gates is more time-consuming, while it only slightly enhances the performance. Therefore, two strategies are combined using 1 AND gate to simulate the following experiments.

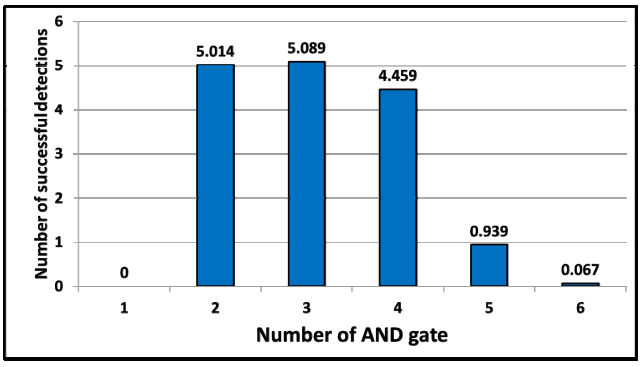

Figure 9. Comparison of the number of successful detections for different numbers of AND gates

4.2.2 Result Comparison and Analysis

This section compares the results obtained using the proposed method with those obtained using [3] and SWAN [9, 22]. First, the three methods are compared with using different numbers of distributed nodes and transmission ranges. Figure 10, Figure 11, Figure 12, and Figure 13 show true negative, false positives, true positive and false negatives, respectively. Since the experimental data from SWAN [9] only provide false positive data, we can only calculate the true negative data, which are presented in Figure 10 and Figure 11. The number of distributed nodes is 150 to 400, with a transmission range of 60 m. SWAN detects wormholes when the number of neighbors is greater than the threshold calculated by a product of value and the mean. Therefore, SWAN will detect erroneously when the distributed nodes decrease, resulting less neighbors. However, as the distributed nodes increase in number, erroneous detections will decrease. In the experimental results in Figure 10, reference [2] and [21] have good performance for true negatives.

The research we proposed has a 100% detection rate in true negatives and will not be affected by the number of nodes. In addition, Figure 11 also shows that our method is superior to other detection methods. Our detection method takes advantage of logic gates and has good performance However, since it is possible to effectively detect that a node goes in and out of a wormhole with different numbers of nodes, so regardless of the number of distributed nodes and its detection rate still maintain 100%.

Figure 14, Figure 15, Figure 16, Figure 17 compare true positive and true negative scores with different transmission ranges. The transmission ranges varied from 40 to 70 m, with 300 distributed nodes. SWAN made erroneous detections when the transmission range decreased, resulting in fewer neighbors. When the transmission range increased, SWANs detection performance improved. Both [2] and the proposed method have good performance for true positive, regardless of the transmission range. However, the true positive rate of [21] decreased when the transmission range increased because the method combined strategies with 2 AND gates, and combined rules with 150 OR gates, while observing the rule base at every step.

When the transmission range increased, the number of nodes being attacked by a wormhole also increased. The detection rate of wormhole has also increased. However, the proposed method uses AND gate and OR gates, and uses the characteristic of being attacked continuously to detect malicious attacks when the node moves into and out of wormhole range. It thus uses fewer logic gates, but still has great performance for true positive and true negative detection with different transmission ranges.

Finally, the required number of OR gates. 100 distributed nodes were used, each with a transmission range of 50 m. The method in [2] maintained the advantages of two kinds of logic gates and used 433 OR gates to combine rules with 100% detection accuracy. The proposed method only used 56 OR gates, but also had 100% detection accuracy. It therefore required far fewer resources than [2], as shown in Table 6. The proposed method makes good use of the characteristic that a node is attacked continuously by malicious nodes when it moves into the wormhole's range, and so significantly reduce the required number of OR gates.

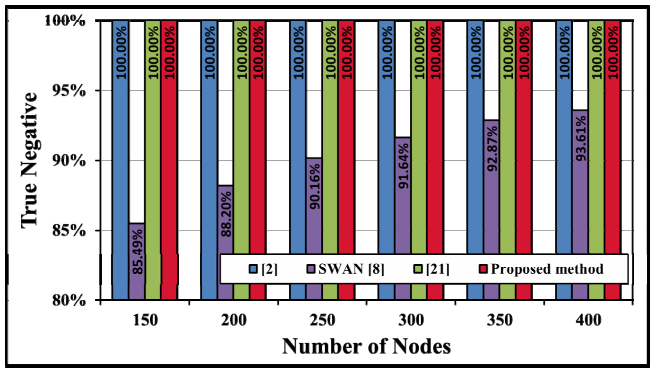

Figure 10. Comparison of TN for different numbers of distributed nodes

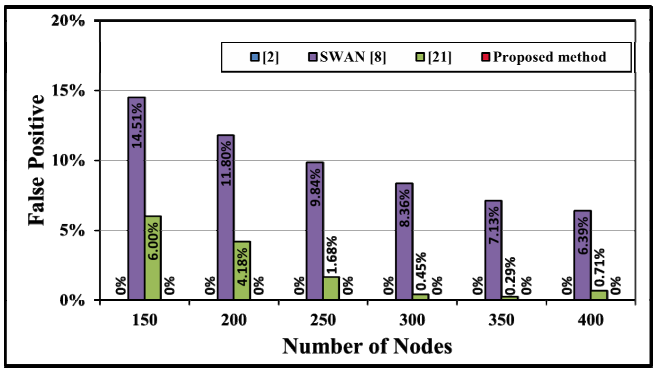

Figure 11. Comparison of FP for different numbers of distributed nodes

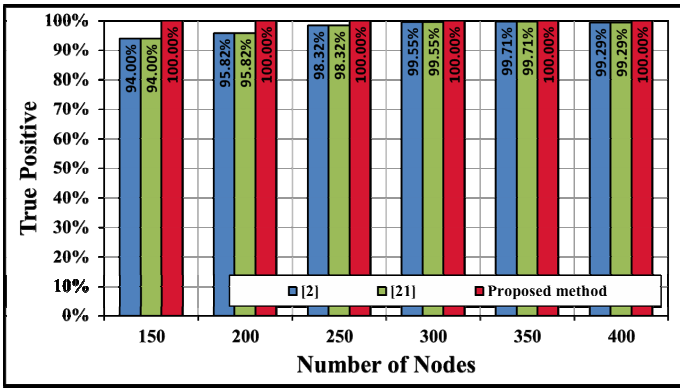

Figure 12. Comparison of TP for different numbers of distributed nodes

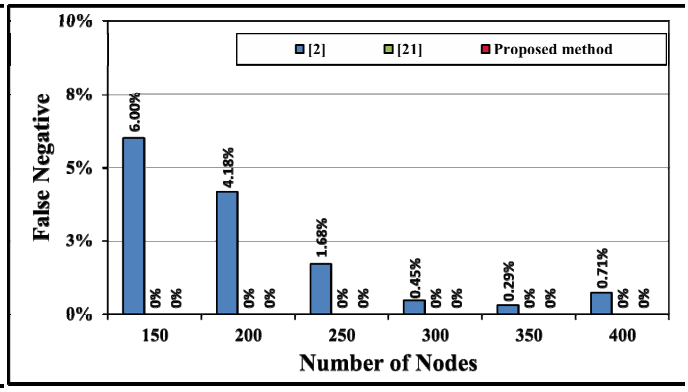

Figure 13. Comparison of FN for different numbers of distributed nodes

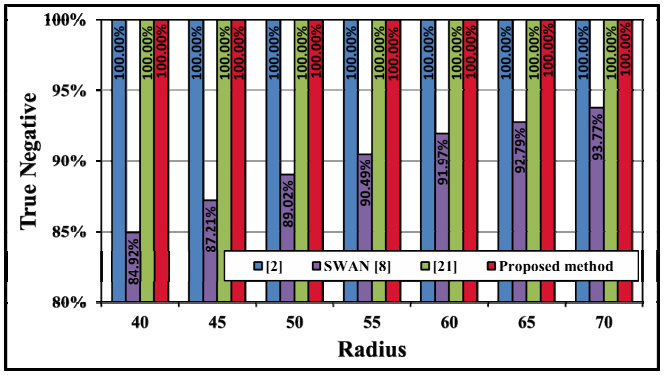

Figure 14. Comparison of TN for different transmission ranges

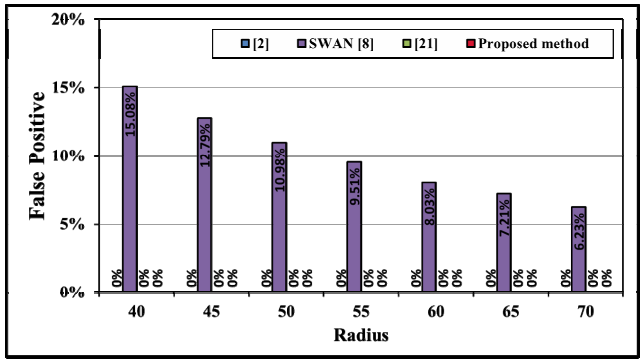

Figure 15. Comparison of FP for different transmission ranges

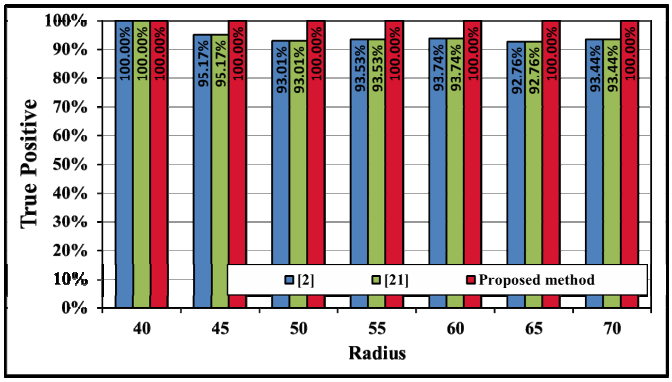

Figure 16. Comparison of TP for different transmission ranges

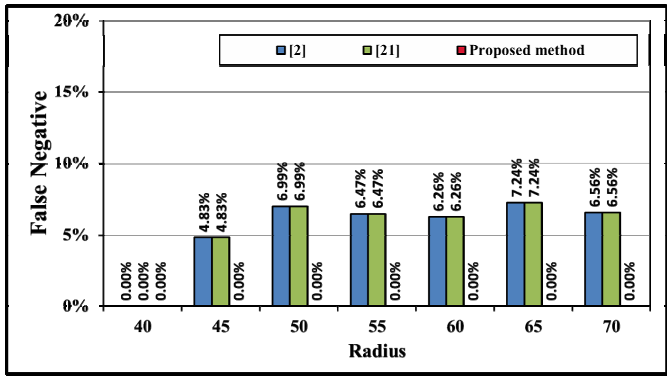

Figure 17. Comparison of FN for different transmission ranges

5 Conclusion

This paper proposes a method for detecting wormhole attacks in WSNs. Without using special hardware devices and complex calculation, MA is used, calculated by the number of node neighbors, and combined with logic operation. AND gates are used to combine two strategies into a rule, so as to make judgments more rigorous. Multiple rules are then combined by OR gates to detect wormhole attacks in different situations. This method makes good use of the characteristic that a node is under constant attack by malicious nodes for as long as it is within their detection range. QTS is then used to find the best rule bases in the vast solution space. The simulation results show that the proposed method effectively reduces the required logic gate resources used to combine rules, and has great performance for different node densities and transmission ranges.However, there are other kinds of MA, such as Weighted Moving Average and Exponential Moving Average, and future research could examine the benefits of these. Future work should explore the use of more generations of interval, greater number of populations.

References

[1] Y. Wang, Z. Zhang, J. Wu, A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information, *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*, Macau, 2010, pp. 63-72.

[2] R.-S. Chang, S.-H. Wang, W.-P. Yang, Addressing Wormhole Attacks on the Internet, *Journal of Internet Technology*, Vol. 13, No. 2, pp. 245-255, March, 2012.

[3] M.-H. Jao, *A Novel Wormhole Attack Detection in WSN: Using Quantum Inspired Tabu Search Algorithm with Logic Operation and Moving Average*, Mater's Thesis, National Chi Nan University, Puli, Taiwan, 2016.

[4] L. Hu, D. Evans. Using Directional Antennas to Prevent Wormhole Attacks, *Network and Distributed System Security Symposium (NDSS 2004)*, San Diego, CA, 2004.

[5] L. Buttyan, L. Dora, I. Vajda, Statistical Wormhole Detection in Sensor Networks, *European Workshop on Security and Privacy in Ad-hoc and Sensor Networks*, Berlin, Heidelberg, 2005, pp. 128-141.

[6] G. N. Shirazi, L. Lampe, Lifetime Maximization of UWB-Based Sensor Networks for Event Detection Applications, *2010 IEEE International Conference on Communications*, Cape Town, South Africa, 2010, pp. 1-6.

[7] Y. C. Hu, A. Perrig, D. B. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks, *Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, San Francisco, CA, 2003, pp. 1976-1986.

[8] D. Dong, M. Li, Y. Liu, X. Y. Li, X. Liao Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, *IEEE/ACM Transactions on Networking*, Vol. 19, No. 6, pp. 1787-1796, December, 2011.

[9] S. Song, H. Wu, B.-Y. Choi, Statistical Wormhole Detection for Mobile Sensor Networks, *2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN)*, Phuket, Thailand, 2012, pp. 322-327.

[10] M. N. A. Shaon, K. Ferens, Wireless Sensor Network Wormhole Detection using an Artificial Neural Network, *Proceedings of the International Conference on Wireless Networks (ICWN)*, Las Vegas, NV, 2015, pp. 115-120.

[11] S. Eidie, B. Akbari, P. Poshtiban, WANI: Wormhole Avoidance Using Neighbor Information, *2015 7th Conference on Information and Knowledge Technology (IKT)*, Urmia, Iran, 2015, pp. 1-6.

[12] T. Chen, H. Huang, Z. Chen, Y. Wu, H. Jiang, A Secure Routing Mechanism Against Wormhole Attack in IPv6-based Wireless Sensor Networks, *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, Nanjing, China, 2015, pp. 110-115.

[13] Y. H. Chou, Y. J. Yang, C. H. Chiu, Classical and Quantum-inspired Tabu Search for Solving 0/1 Knapsack Problem, *2011 IEEE International Conference on Systems, Man, and Cybernetics*, Anchorage, AK, 2011, pp. 1364-1369.

[14] W. H. Wang, C. H. Chiu, S. Y. Kuo, S. F. Huang, Y. H. Chou, Quantum-Inspired Tabu Search Algorithm for Reversible Logic Circuit Synthesis, *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Seoul, South Korea, 2012, pp. 709-714.

[15] Y. J. Yang, S. Y. Kuo, F. J. Lin, I. I. Liu, Y. H. Chou, Improved Quantum-Inspired Tabu Search Algorithm for Solving Function Optimization Problem, *2013 IEEE International Conference on Systems, Man, and Cybernetics*, Manchester, UK, 2013, pp. 823-828.

[16] Y. H. Chou, S. Y. Kuo, C. Kuo, Y. C. Tsai, Intelligent Stock Trading System Based on QTS Algorithm in Japan's Stock Market, *2013 IEEE International Conference on Systems, Man, and Cybernetics*, Manchester, UK, 2013, pp. 977-982.

[17] S. Y. Kuo, C. Kuo, Y. H. Chou, Dynamic Stock Trading System Based on Quantum-inspired Tabu Search Algorithm, *2013 IEEE Congress on Evolutionary Computation*, Cancun, Mexico, 2013, pp. 1029-1036.

[18] Y. H. Chou, S. Y. Kuo, C. Y. Chen, H. C. Chao, A Rule-based Dynamic Decision-making Stock Trading System Based on Quantum-Inspired Tabu Search Algorithm, *IEEE Access*, Vol. 2, pp. 883-896, September, 2014.

[19] Y. H. Chou, S. Y. Kuo, C. Kuo, A dynamic stock trading system based on a Multi-objective Quantum-Inspired Tabu Search Algorithm, *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, San Diego, CA, 2014, pp. 112-119.

[20] C. Bettstetter, G. Resta, P. Santi, The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks, *IEEE Transactions on Mobile Computing*, Vol. 2, No. 3, pp. 257-269, July-September, 2003.

[21] B. Chen, A. Phillips, T. I. Matis, Two-terminal Reliability of

a Mobile Ad Hoc Network under the Asymptotic Spatial Distribution of the Random Waypoint Model, *Reliability Engineering and System Safety*, Vol. 106, pp. 72-79, 2012.

[22] M.-H. Jao, M.-H. Hsieh, K.-H. He, D.-H. Liu, S.-Y. Kuo, T.-H. Chu, Y.-H. Chou, A Wormhole Attacks Detection Using a QTS Algorithm with MA in WSN, *2015 IEEE International Conference on Systems, Man, and Cybernetics*, Kowloon, China, 2015, pp. 20-25.

Biographies

Ting-Hui Chu is a Ph.D. student at the Department of Computer Science and Information Engineering of National Chi Nan University. His research interests include VANET, wireless sensor network, and sensor network security.

Shu-Yu Kuo is a Ph.D. student at the Department of Computer Science and Information Engineering of National Chi Nan University. Her research interests include wireless sensor network, deployment system, and evolutionary computation.

Yao-Hsin Chou received his Ph.D. degree from the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan, in 2009. He is currently an Associate Professor with the Department of Computer Science and Information Engineering, National Chi Nan University, Nantou, Taiwan. He has authored over 60 papers in journals and conference proceedings. His current research interests include wireless sensor network, network security, artificial intelligence, and quantum information science.