IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 December 2023, accepted 12 January 2024, date of publication 18 January 2024, date of current version 2 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3355467

RESEARCH ARTICLE

Trust System- and Multiple Verification Technique-Based Method for Detecting Wormhole Attacks in MANETs

JOONSU RYU, (Graduate Student Member, IEEE), AND SUNGWOOK KIM
Department of Computer Science, Sogang University, Mapo-gu, Seoul 04107, South Korea

Corresponding author: Sungwook Kim (swkim01@sogang.ac.kr)

This work was supported in part by the Ministry of Science and ICT (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program, Supervised by the Institute of Information and Communications Technology Planning and Evaluation (IITP), under Grant IITP-2023-2018-0-01799; and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2021R1F1A1045472.

ABSTRACT The proliferation of wireless mobile devices has resulted in mobile ad hoc network (MANET) technologies, which enable the formation of networks without infrastructure assistance, gaining increased attention. The advancements in these technologies have also resulted in the variety of attacks targeting them becoming more diversified. Particularly, owing to their inability to ensure node reliability, MANETs are vulnerable to routing attacks such as wormhole attacks. Since wormhole attacks often do not directly damage networks, detecting them can be challenging. In response, we propose a novel multiple verification-based wormhole attack detection method that leverages the characteristics of such attacks. The proposed method measures the credit of each node based on a trust system. The trust levels of suspicious nodes are reduced during routing; those with trust levels below a certain threshold are considered malicious. This trust system was implemented using reinforcement learning, which improves the accuracy of the system over time. Simulation experiments in which the proposed method was applied to existing routing methods in a densely populated environment were conducted; the rate of traffic passing through paths with malicious nodes was significantly reduced.

INDEX TERMS Incentive mechanism, mobile ad-hoc network, reinforcement learning, wormhole attack.

I. INTRODUCTION

In recent years, the adoption of wireless terminal devices has skyrocketed, resulting in an increased demand for advanced network technologies that enable communication without the need for traditional infrastructure. A representative technology that has come to the forefront is the mobile ad hoc network (MANET) [1]. Unfortunately, the increased sophistication of this technology has resulted in a corresponding increase in the range and complexity of potential attacks, posing significant challenges to network security [2].

One of the key vulnerabilities of MANETs is their inability to effectively handle node failures, which makes them particularly susceptible to routing attacks such as wormhole attacks [3]. In these attacks, packets are forwarded between malicious nodes using a secret path called a tunnel. These malicious nodes connected through the tunnel disguise themselves as neighboring nodes and induce legitimate neighboring nodes to transmit their packets. Since such a tunnel has a high bandwidth and enables packets to travel longer distances than other routes do, neighboring nodes incorrectly judge the path to be more efficient for packet transmission [4]. Although a wormhole attack does not directly damage a network—in terms of resulting in an increased packet loss rate or energy consumption—like a black hole attack or gray hole attack does [5], it poses the risk of lowering network stability and causing severe damage through follow-up attacks [6]. Therefore, there is an urgent need for effective detection and mitigation strategies against

The associate editor coordinating the review of this manuscript and approving it for publication was Zesong Fei.

these types of attacks to ensure the integrity and reliability of MANETs.

Thus, we propose a wormhole attack detection method, which employs a multiple verification technique that exploits the characteristics of these attacks. The core functionality of this method is a trust system, which measures the reliability of each node and identifies potentially malicious nodes. The role of reinforcement learning and incentive mechanisms in implementing this trust system was explored in the study. The proposed approach can provide improved accuracy over time and overcome the challenge of false alarms, which is a common issue in attack detection systems [7].

Reinforcement learning offers a dynamic approach to learning optimal strategies based on experiences. It is a type of machine learning strategy in which an agent interacts with an environment and learns how to make decisions that maximize the cumulative rewards [8]. Nodes that act as agents in wormhole detection can identify suspected malicious nodes based on historical data, thereby improving their ability to identify and respond to latent threats. This learning ability enables significant improvements in wormhole detection over time.

An incentive mechanism is a systematic process or method that motivates a shift in the behavior of individuals or groups toward a desired direction [9]. The incentive mechanism can be used to induce cooperation between nodes against malicious attacks such as wormhole attacks. For example, an incentive mechanism can be introduced in the process of strengthening network security to enable nodes to jointly develop ways to prevent or respond to attacks [10]. Through this mechanism, nodes can cooperate and share information, which is beneficial to individual interests. Consequently, the safety of the entire network can be enhanced. Incentives can be provided in the form of additional rewards to nodes that succeed in preventing or responding to attacks, encouraging cooperation and suppressing malicious behavior. In this way, the incentive mechanism can be effectively utilized to enhance security against malicious attacks and induce cooperation among nodes.

By combining reinforcement learning and an incentive mechanism, a powerful combination of strategic decision-making and dynamic learning suitable for detecting and responding to wormhole attacks in MANETs [11], [12], [13] can be created. This combination is an innovative contribution to the proposed trust system, which aims to improve the security of MANETs.

The main contributions of this paper are summarized as follows:

1. This paper proposes a novel trust system that leverages reinforcement learning and an incentive mechanism to detect wormhole attacks in MANETs. The trust of a node is measured based on the characteristics of the wormhole attack. If the trust of a node drops below the threshold value, the network excludes it from the network, thereby ensuring security.
2. The proposed method can effectively respond even in dynamic network environments such as MANETs. Furthermore, it can detect malicious nodes regardless of their type, including ones that use an isolated channel.
3. The proposed method can be applied to existing routing protocols such as Dynamic Source Routing (DSR) [14], Ad hoc On-demand Distance Vector routing (AODV) [15], and Opportunistic Routing (OR) [16], without the need for any special accessory devices. This means that it can be applied flexibly regardless of the type of routing protocol employed by a MANET.

The remainder of this paper is structured as follows. Section II reviews related work on this subject, including countermeasures for wormhole attacks. Then, Section III describes the network and attack models used in this study, and Section IV introduces the proposed key method, details its design, and describes its approach to wormhole attack detection. After that, Section V presents the simulations performed to evaluate the effectiveness of the proposed method in comparison with other wormhole detection methods in various routing protocols. Finally, Section VI concludes the paper and discusses the limitations of the study.

II. RELATED WORKS

This section summarizes existing countermeasures against wormhole attacks and describes their drawbacks and limitations. Hu et al. [17] proposed a wormhole attack detection mechanism using packet leashes. This method involves calculating the distance to the sending node and the time required for the packet to traverse the path, which is done to verify whether the packet receiver is within a certain distance from the sender. Through this, it can be verified whether the packet is passing through a wormhole tunnel when traveling a long distance. This method operates under a constraint that specifies that the time required for all the nodes should be accurately synchronized.

Chiu and King-Shan [18] designed the delay per hop indication (DelPHI), a method for detecting wormhole attacks by calculating the round-trip time (RTT). This method calculates the packet-delivery delay at each hop and appends it to the corresponding packet. If the packet traverses a long distance in a short period, it indicates a potential wormhole attack. This method can be implemented without additional hardware; however, like with the packet leash-based method, accurate time synchronization is necessary.

Čapkun et al. [19] introduced a wormhole attack detection method called secure tracking of node encounters (SECTOR). Unlike the packet leash-based method and DelPHI, SECTOR does not require time synchronization. It calculates the actual distance between two nodes by exchanging special bits between them and calculating the RTT. If the distance is longer than that between the neighboring nodes, it indicates malicious behavior. This method is limited in that it requires separate specialized hardware to exchange the special bits.

Hu and Evans [20] proposed a method for detecting wormhole attacks using directional antennas. This method exploits the characteristic of wireless signals needing to be received in a specific direction. The authors designed a system in which the direction of the signals received from any neighboring nodes was detected through directional antennas. If the packets were received from an unexpected direction, the corresponding node was deemed malicious and excluded from the network. This method requires that all nodes should be equipped with directional antennas.

Khalil et al. [21] studied a method called lightweight wormhole attack detection and prevention (LITEWORP) that utilizes neighboring nodes for wormhole attack detection. In LITEWORP, each node communicates with the neighboring nodes and builds a routing table; when packets travel through unexpected routes, it is determined that a wormhole attack has occurred, and nodes suspected of being malicious are blocked. This method is effective in infrastructure-less communication technologies, such as MANETs. However, it has a drawback in that all the nodes in the network should precisely know their locations. Additionally, detection is infeasible if malicious nodes propagate false neighbor information during the creation of the routing table.

Van Tran et al. [22] suggested a transmission time-based mechanism (TTM) that detects wormhole attacks using the time difference between route request (RREQ) and route reply (RREP) messages in the AODV routing protocol. If the RTT calculated based on the RREQ and RREP is below a certain threshold, a wormhole attack is judged to have occurred. The TTM allows for the simple detection of wormhole attacks without the need for additional hardware or complex calculations. However, incorrect judgments may potentially occur depending on the network situation, and unfortunately, malicious nodes can manipulate time information during routing.

Chen et al. [23] proposed a wormhole detection technique based on distance consistency. Existing wormhole attack detection methods that are based on the Global Positioning System (GPS) encounter the problem of malicious nodes manipulating their locations to evade wormhole attack detection. This method can resolve this issue by accurately identifying the locations of nodes using localization techniques. However, it is limited in that it only functions correctly in environments without packet losses.

Biswas et al. [24] designed a wormhole attack detection and prevention (WADP) technique capable of detecting wormholes using the AODV protocol. This technique employs node authentication to solve the false-positive problem inherent in wormhole detection methods. Advantageously, it can accurately map the location of a wormhole without the need for special hardware. However, it is difficult to apply this method to routing protocols other than AODV, and the verification-based need to update the information between nodes in real time can increase the burden on the network.

Jamali and Fotohi [25] introduced a method that uses an artificial immune system (AIS) to prevent wormhole attacks without degrading network performance. This method sends test packets to each path and requests the confirmed packets. If a tunnel exists on the path, the test packet will not reach its destination; thus, the confirmation packet will not arrive, and the path will not be selected. However, this method has a drawback in that it is likely to choose inefficient paths because it deliberately excludes paths with a small number of hops.

Verma et al. [26] presented a wormhole attack detection method using packet delivery ratio (PDR) and RTT for nodes. If the RTT of the node is below the specified threshold, it is indicative of a wormhole attack. Additionally, this method measures the PDR to ascertain the type of wormhole attack; if it is less than 1, it is active, and if it is greater than 1, it is passive. The advantage of this method is that it can detect the attack methods of malicious nodes. Since it is an RTT-based method, it cannot perform detections in situations where an accurate RTT cannot be measured owing to packet loss or packet manipulation.

Shukla et al. [27] studied a method that uses a cryptographic technique to mitigate the damage caused by black hole and wormhole attacks. This method uses elliptical curve cryptography, which can provide security levels that resemble those of Rivest-Shamir-Adleman (RSA) and can be easily analyzed externally. However, there is a drawback in that the additional cost required for the necessary encryption and decryption concerns a mobile environment with limited computational and energy resources.

Han et al. [28] suggested a wormhole attack detection algorithm called the distance vector hop localization algorithm (ANDV-Hop), which is an improvement on the distance vector hop (DV-Hop) algorithm that determines the location of sensor nodes in sensor networks and detects wormhole attacks by exploiting the characteristic of sensor nodes not receiving the same data packet again. However, this method can only be used in sensor networks and, even within these networks, detecting whether a sensor node is reinitialized is challenging due to environmental or other unforeseen factors.

Abdan and Seno [29] used various machine learning algorithms to classify malicious nodes. Their approach involved identifying the characteristics of malicious nodes based on the node data collected, followed by simulations conducted using MATLAB 2019b. They found that the decision tree (DT) algorithm achieved a detection accuracy as high as 98.9%. However, the application of this method requires collecting data from the entire network, which can be difficult in a MANET environment comprising independent nodes.

Additionally, various methods have been proposed to detect and mitigate wormhole attacks [30], [31]. However, each method has limitations, including the need for specific hardware, high computational complexity, and dependence on a specific network structure; new methods that overcome

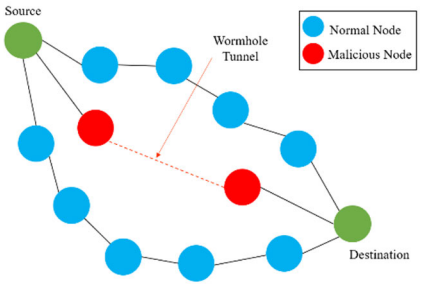


FIGURE 1. Example of a wormhole attack in a mobile ad hoc network (MANET).

these limitations should be developed. The goal of the current study is to solve these problems and propose a more effective and practical method for detecting and defending against wormhole attacks.

III. SYSTEM MODEL

This section details the network and attack models used in this study. These models provide a foundation for understanding the use of the proposed method for detecting and defending against wormhole attacks. Fig. 1 illustrates the wormhole attack mechanism.

A. NETWORK MODEL

In the study, it was assumed that a MANET comprised only dynamic normal nodes. The positions of the nodes were initialized randomly, and the movement of each node followed the random-walk 2D model [32], assuming that the nodes moved at speeds of 0–5 m/s. Additionally, the communication range of each node was the same, and bidirectional communication (communication from node A to node B and node B to node A) was possible.

In the study, reactive routing (i.e., on-demand routing) and OR were assumed to be the routing protocols for a MANET. Reactive routing is a method that only finds a routing path when there is a need to send a packet, that is, when a request is made. It is a widely used routing technique in dynamic network environments such as MANETs, where the connectivity between nodes changes frequently [33].

Regarding DSR, it is a representative reactive routing method [14] where the source node sets the entire path to the destination in the packet and includes this path information in the packet. It uses RREQ and RREP messages to include the path information in all the packets, provided the path is known by the source node. Therefore, each node can know the path information of the packet reaching it, advantageously reducing the packet propagation required to find other paths.

Another popular reactive routing protocol is AODV [15], which can respond flexibly to rapid changes in the network structure by updating the routing table according to changes in the network configuration. This protocol also uses RREQ and RREP. When a node wants to send a packet to a destination, it determines the path to the destination in the routing table. If a path does not exist, it initiates route discovery through an RREQ message. This message is then propagated throughout the network until it is received by a destination node or an intermediate node that contains information about the path. When the path is found, the RREP message is returned to the source node, updating it with the path information.

Regarding OR, it is a strategy for improving the packet transmission in MANETs [16]. Unlike DSR or AODV, this strategy selects the optimal node among multiple candidate nodes for sending a packet. This selection process considers various factors, such as the communication status, location, and energy status of a node. When one of the candidate nodes successfully receives the packet, a signal is sent to the remaining candidate nodes to cancel packet transmission, thereby reducing the occurrence of duplicate transmissions and improving communication efficiency.

B. ATTACK MODEL

As shown in Fig. 1, in a wormhole attack, two malicious nodes create a tunnel between them and intercept, forge, or alter packets passing through this path, thereby indirectly harming the network [17]. These attacks can be classified into in-band and out-of-band attacks [34].

In an in-band wormhole attack, an attacker forwards packets over a typical wireless connection used in a network. Tunnels connected between malicious nodes are disguised as more efficient routes and induce network traffic from other nodes. In out-of-band wormhole attacks, malicious nodes forward packets using a dedicated communication channel, which employs a wired connection or a wireless connection with a higher bandwidth. Like the connection in an in-band wormhole attack, these dedicated channels can attract traffic from other nodes because they are faster and more efficient than other routes.

Thus, regardless of the wormhole attack type, the malicious nodes create a tunnel between two locations and make the path between them appear more efficient than other routes, enabling the node to collect more packets [35]. Therefore, in this study, we did not consider the common assumption that such a tunnel has a poorer communication quality than that of a normal route [36]. In wormhole attacks, malicious nodes need to maintain high communication quality in the tunnels they create. If these nodes are dynamic, the complexity of the attack increases, considering the stringent levels of synchronization and management required [37]. Therefore, we assumed that the malicious nodes, unlike the other nodes, were static. Additionally, the creation of false routes in wormhole attacks can potentially cause confusion in the network structure and routing protocol or lead to subsequent attacks, such as denial of service (DoS) [38].

IV. PROPOSED METHOD

This section introduces the proposed wormhole detection technique. This technique exploits the unique characteristics of wormhole attacks, making it a specialized and effective

approach for detecting and mitigating the threats posed by them. Our proposed technique provides a robust and adaptable solution for ensuring security in MANETs that aims to overcome the limitations of existing methods. Regarding its working, it uses reinforcement learning to learn the trust levels of nodes. Under this method, the reward is computed based on the results of multiple verifications. If the learned trust level of a node falls below a certain threshold, the network considers that node as malicious and excludes it to establish a safe communication environment.

The basic concept of reinforcement learning is discussed here. It is a type of machine learning method in which an agent learns to make decisions by interacting with the environment [10]. Reinforcement learning can be modeled as a Markov decision process (MDP); the MDP used in this study is defined as a 4-tuple $\langle S, A, P, R\rangle$ as follows:

- S is a finite set of states; here, it is equal to the set of all nodes.
- A is the finite set of actions; here, it is equal to the set of all nodes.
- P is a state-transition probability matrix that indicates the probability of transitioning to the next state when an action is selected in the current state. In this study, the choice of action is governed by the given routing protocol; therefore, it is not addressed here.
- R is the reward function, meaning that feedback is obtained when an action is selected in its current state; here, it refers to the updated trust levels.

A representative reinforcement learning method is Q-learning [39], which is a value-iteration algorithm in reinforcement learning. In Q-learning, the agent learns an action-value function that represents the expected utility of performing a given action in a particular state, considering the future rewards. The updated equation for Q-learning can be expressed as:

$$Q(s_t, a_t) \leftarrow (1-\alpha)\, Q(s_t, a_t) + \alpha\left[r_{t+1} + \gamma Q(s_{t+1}, a)\right], \tag{1}$$

where s_t and a_t represent the state and action at time t, respectively; $\alpha \in [0, 1]$ denotes the learning rate; r_{t+1} is the reward obtained as a result of the state s_t and action a_t; and $\gamma \in [0, 1]$ is the discount factor. Equation (2) represents the validation method when the communication range of a tunnel in a wormhole attack is considered typically longer than the wireless communication range of regular nodes [40]:

$$T_A(s_0, s_t) = \frac{hop_{real}(s_0, s_t) - hop_{ideal}(s_0, s_t)}{hop_{real}(s_0, s_t)}, \tag{2}$$

where s_0 is the first source node of the packet , s_t is the node that currently has the packet, $hop_{ideal}(s_0, s_t)$ is the minimum number of hops required to communicate from s_0 to s_t, and $hop_{real}(s_0, s_t)$ is the actual number of hops taken to communicate from s_0 to s_t.

Fig. 2 (a) schematically depicts the minimum number of hops spanning the boundaries of the communication range. In general communications, more hops are required, as shown in Fig. 2 (b). Therefore, if the T_A value in Equation (2) is close to 0, it indicates the presence of a potential tunnel in the path.

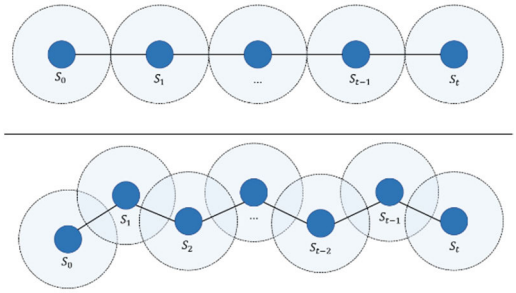


FIGURE 2. Example of ideal (above) and actual (below) number of hops taken for communication.

The second component in wormhole attack detection involves checking the number of times a path between certain nodes is selected during the routing process. Since the MANET considered in the study comprised only dynamic nodes, the network structure was subject to change at any time. Malicious nodes that conduct a wormhole attack are not separate wireless nodes but interconnected ones; thus, they transmit most or all the packets through the tunnel. Since a pair of malicious nodes is statically connected, the likelihood that the nodes exchange packets more frequently than other nodes do is high [41]. The second component in wormhole attack detection is represented as follows:

$$T_B(a, b) = \begin{cases} e^{-c\times(path(a,b)-path_{avg})}, & if\ path_{avg} < path(a, b) \\ 1, & otherwise, \end{cases} \tag{3}$$

where $path_{avg}$ is the average number of paths used in the entire network, and $path(a, b)$ is the number of times node a uses a path connected to node b. $c > 0$ is a constant depending on the network. When the value of T_B decreases, it indicates that there is a high probability of a tunnel existing in the path between nodes a and node b.

The third component in wormhole attack detection involves exchanging forwarding information with neighboring nodes when transmitting packets. Fig. 3 depicts a situation in which node M1 sends a packet to node M2 through a wormhole tunnel. Since a wormhole tunnel can transmit data over longer distances or through a dedicated channel, the nodes around M2 cannot receive packet transmission signals. Nodes A and B, which are neighbors of node M2, are closer to node M1 than they are to node M2. Thus, if the communication between M1 and M2 is normal in the network, the transmission signal should also reach nodes A and B. However, since the communication is through a tunnel, as shown in Fig. 3, nodes A and B cannot receive this signal. This means that if the neighboring nodes of the packet receiving the node cannot receive a packet reception signal, a wormhole attack can occur [42]. The third component of wormhole attack

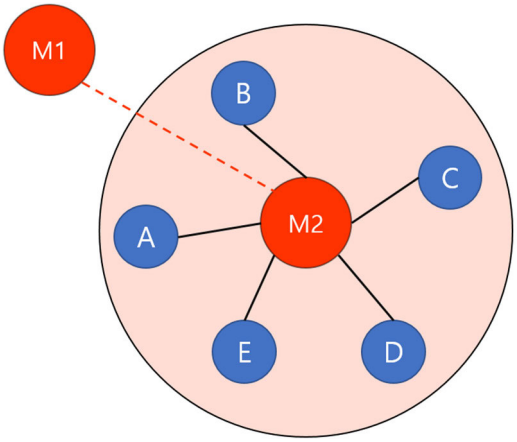


FIGURE 3. Communication between malicious nodes M1 and M2 using a tunnel and their surrounding nodes.

detection can be expressed as:

$$T_C\,(a,b) = \min\left[\frac{N\,(a,b)}{N_{avg}}, 1\right], \tag{4}$$

where $N\,(a,b)$ is the number of neighboring nodes of node b that receive the signal when a packet is transferred from node a to node b, and N_{avg} is the average number of neighboring nodes among the receiving nodes that receive packet-forwarding signals. If the value of T_C is approximately 0, the packet is highly likely to have been transmitted through the tunnel between nodes a and node b.

Based on Equations (2)–(4), r_{t+1} in Equation (1) can be defined as follows:

$$r_{t+1} = w_1 \times T_A\,(s_0, s_t) + w_2 \times T_B\,(s_{t-1}, a_{t-1}) + w_3 \times T_C\,(s_{t-1}, a_{t-1}), \tag{5}$$

where w_1, w_2, and w_3 are the weights of each component; $w_1 + w_2 + w_3 = 1$. The weight of each component can be set differently based on the network environment. For example, in a network with sparse nodes, the number of hops in routing may decrease. Therefore, reducing the weight of w_1 allows for more accurate verification. The Q-value learned through Equation (5) indicates the trust in the path between two nodes. If the Q-value learned in this manner falls below the threshold value, the two nodes are considered malicious nodes performing a wormhole attack and are excluded from the network. The threshold used for node verification can be set differently based on the network structure. For instance, in environments with high node densities, the possibility of variables used in the reward function being inaccurately measured because of packet loss is relatively low. In such cases, the threshold can be set to a relatively low value. This process of wormhole attack detection can be represented in the pseudocode given below.

In this algorithm, the Q values are updated after each packet is forwarded to the next node. First, in line 6, the node that receives the packet observes the previous states s_{t-2} and s_{t-1}

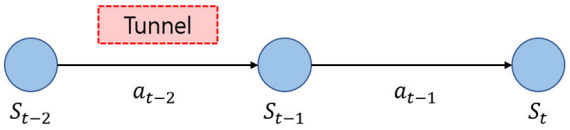


FIGURE 4. Verification process of the proposed algorithm.

and the action a_{t-2}. Then, it computes the rewards using the proposed verification method represented in lines 7–10. Subsequently, it updates the Q value as shown in line 11 and checks whether the trust in the path is below the threshold using the if statement from lines 12–14. If the value of a node is below the threshold, it is excluded from the network. Here, because the MANET does not have a central control device to process this information, it broadcasts it to the neighboring nodes. As mentioned in line 15, the constant values are updated as necessary for verification, and as described in lines 16–17, the packet is then forwarded to the next node. The proposed algorithm repeats this process, checking for the presence of malicious nodes on a path until the packet reaches its destination.

Algorithm 1 Wormhole Attack Detection Based on Trust Level

Input: Parameters α, γ the threshold, w_1, w_2, w_3 and the routing protocol
Output: A network comprising only trusted nodes

1: Q ← initialize Q value for all $s \in \mathcal{S}$, $a \in \mathcal{A}\,(s)$
2: π ← given routing protocol
3: **Loop** for each packet **do**
4: Determine the source node s_0 and destination node s_d
5: **while** packet has not reached destination **do**
6: Observe the previous state s_{t-2} and s_{t-1} and the previous action a_{t-2}
7: Calculate $T_A\left(s_0, s_{t-1}\right)$ using Equation (2)
8: Calculate $T_B\left(s_{t-2}, a_{t-2}\right)$ using Equation (3)
9: Calculate $T_C\left(s_{t-2}, a_{t-2}\right)$ using Equation (4)
10: Calculate r_t using Equation (5)
11: Update $Q\left(s_{t-2}, a_{t-2}\right)$ using Equation (1)
12: **if** $Q\left(s_{t-2}, a_{t-2}\right) <$ threshold
13: **then** exclude node s_{t-2} and s_{t-1} from the network
14: **end if**
15: Update $path_{avg}$ and N_{avg}
16: Choose action a with policy π
17: Move to next state s_{t+1}
18: **end while**
19:**end Loop**
20:**end**

The proposed algorithm is designed such that current node s_t verifies nodes s_{t-2} and s_{t-1}. As shown in Fig. 4, if node s_{t-1} is a malicious node, node s_{t-1} forwards the packet from node s_{t-2} through the tunnel. Because a malicious node will not reveal itself as such, the algorithm is designed to enable verification by the adjacent node instead.

When a packet is forwarded to the next node, the proposed method is immediately activated, thus enabling real-time detection of potential wormhole attacks during the routing process. Despite the complexity involved in this detection

procedure, equations (2)–(4) are intentionally structured so that their parameters can be readily accessible during routine routing operations. Consequently, the computational demand and routing overhead introduced by our method are negligible and can be effectively disregarded. This strategic design guarantees that the proposed method can be seamlessly incorporated into existing MANET infrastructures without imposing a significant burden on network performance.

However, even if a node verifies a malicious node, passing this information on to other nodes is another challenge. This is because notifying other nodes of the presence of a malicious node requires a node to use its own resources (e.g., battery). Therefore, a node will not propagate information about a malicious node without an appropriate payoff for passing on the information.

To encourage each node in the proposed system to propagate verification results to other nodes, an incentive is provided to the node when successful dissemination of information about malicious nodes occurs. The incentive is granted through an increase in the trust value. Specifically, when a node (denoted as node a) possessing information about malicious nodes successfully propagates this information to another node b, the trust value of node a is adjusted using the following equation:

$$Q(a, b) = \min\left[Q(a, b) + \beta Q_{new}, 1\right], \tag{6}$$

where Q_{new} is the additional trust value as an incentive and β is a constant that adjusts the value of Q_{new} based on the network condition. The min operation ensures that the value of $Q(a, b)$ does not exceed 1. Q_{new} is calculated as the sum of the distances between nodes a and b and between the malicious node and node b, as follows:

$$Q_{new} = \frac{D(a, b)}{D_{max}} + \frac{D(m, b)}{D_{max}}, \tag{7}$$

where D_{max} is the maximum distance between two nodes, and $D(a, b)$ and $D(m, b)$ are the distances between nodes a and b and between the malicious node and node b, respectively.

As a culmination of the devised incentive scheme, nodes that propagate information about malicious entities stand to augment the level of trust within the network. This elevated trust, attributed as an incentive, affords these nodes an enhanced packet delivery priority. Consequently, nodes voluntarily adhere to the proposed verification approach in their pursuit of higher trust and priority, thus fostering a network environment where the propagation of verification methods becomes an inherently cooperative endeavor [43], [44].

V. PERFORMANCE EVALUATION

This section details the series of simulation experiments conducted using various routing protocols to verify the effectiveness of the proposed wormhole detection method. These experiments aimed to measure the extent to which the proposed method could mitigate the effect of wormhole attacks. The experiments were crucial to understanding how the proposed algorithm responded to and evaded wormhole attacks in actual network environments.

TABLE 1. Simulation parameters.

Parameters	Values
Network area	1000 × 1000 m
Number of nodes	300
Number of malicious nodes	2
Communication range	100 m
Moving speed of the nodes	0–5 m/s
Size of each packet	1 MB
Buffer size of each node	100 MB
Packet generation rate	1 packet/s
Simulation time	2000 s

The damage caused by wormhole attacks cannot be easily quantified in terms of conventional routing performance metrics such as packet delivery rate or end-to-end delay. Therefore, in this study, we conducted experiments that compared the performances of the existing original routing method, routing protocol incorporating the proposed method, and routing protocol that employed an AIS-based wormhole detection method [25] in the same network environment. The performance measurement criterion was the ratio of packets passing through the wormhole tunnel to the total number of packets delivered to the network. Like the proposed method, the AIS-based wormhole detection method chosen for comparison could be applied regardless of the routing protocol, making it suitable for comparison purposes.

The simulation was implemented using Python software, which has a rich library for such network simulations and an easy and intuitive syntax structure that supports the effective implementation of complex network algorithms. Moreover, the dynamic nature of Python is advantageous for rapid prototyping and simple testing in various scenarios.

A. SIMULATION CONFIGURATIONS

All the nodes except the malicious nodes were initially set with a battery level of 100%, and this level was assumed to only decrease; the malicious nodes capable of battery charging were assumed to have infinite battery capacities and no such charge level limitations. The primary variables used in the simulations are listed in Table 1.

B. SIMULATION RESULTS

To compare the performances of the proposed method, AIS-based wormhole detection method, and normal routing algorithm, we measured the ratio of the number of packets that passed through the wormhole tunnel during the simulation.

Fig. 5 shows the ratio of packets passing through the wormhole tunnel when using the DSR protocol. First, when a normal DSR routing protocol was used in the assumed network environment, approximately 80% of the packets passed through the wormhole tunnel. Then, in the AIS-based wormhole detection method, the ratio decreased with time,

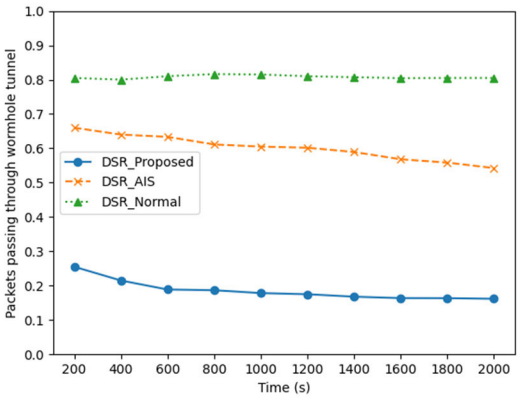


FIGURE 5. Ratio of the packets passing the wormhole tunnel under the dynamic source routing (DSR) protocol.

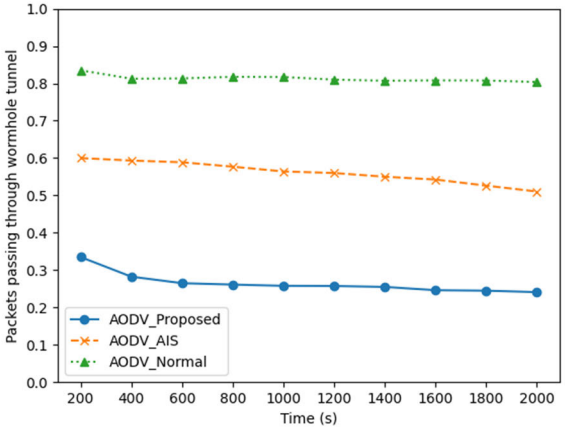


FIGURE 6. Ratio of the packets passing the wormhole tunnel under the ad hoc on-demand distance vector routing (AODV) protocol.

with approximately 54% of the packets passing through the tunnel until the simulation ended. Finally, in the proposed method, approximately 25% of the packets initially passed through the wormhole tunnel; however, as the Q-learning progressed, approximately 16% finally converged to pass through the wormhole tunnel. The proposed method took approximately 600 seconds to converge in the DSR protocol. In summary, this simulation provided further evidence of the vulnerabilities of the conventional DSR protocol to wormhole attacks, as a significant portion of packets opted for the wormhole tunnel as their route. Despite this, the proposed method proved remarkably capable of mitigating such a security threat, resulting in substantial reductions in the percentage of packets routed through the wormhole tunnel. This underscores the potential of the proposed approach to significantly enhance the security and resilience of ad hoc networks based on the DSR protocol.

Fig. 6 illustrates the ratio of packets passing through the wormhole tunnel when using the AODV protocol. Like DSR, this protocol also considered the wormhole tunnel as a superior route and, consequently, approximately 80% of the packets passed through the tunnel. The AIS-based wormhole

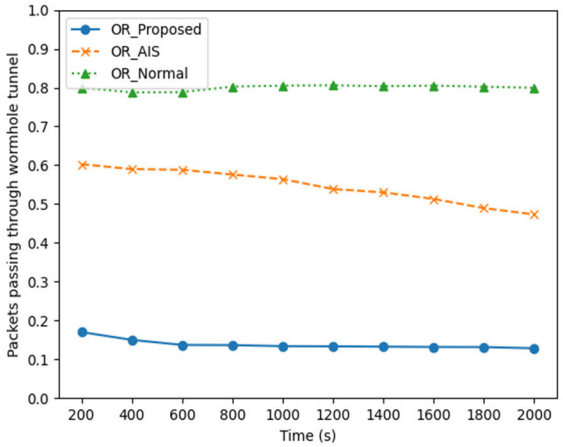


FIGURE 7. Ratio of the packets passing the wormhole tunnel under the opportunistic routing (OR) protocol.

detection method reduced the percentage of packets passing through the wormhole tunnel compared to those under the normal AODV; however, approximately 51% of the packets still passed through the wormhole tunnel. Since the proposed method used Q-learning, the packets initially passed through the wormhole tunnel at a high rate. However, after Q-learning progressed, only approximately 24% of the packets passed through the wormhole tunnel. The proposed method took approximately 600 seconds to converge in the AODV protocol. Overall, the results indicate the potential of the proposed method to substantially enhance the security of the AODV protocol against wormhole attacks. By using past experiences to dynamically adjust routing decisions, the proposed method demonstrated its potential as a robust solution to safeguard ad hoc networks from wormhole threats while minimizing the exposure of packets to vulnerable paths.

Fig. 7 shows the comparison of the performances of the different OR-based protocols. Under the normal OR protocol, without countermeasures against wormhole attacks, approximately 80% of the packets passed through the wormhole tunnel as they did under the other routing protocols. The performance of the AIS-based wormhole detection method did not significantly differ from that of the previous methods, while the proposed method showed the best performance. As in the previous cases, the proposed method took approximately 600 seconds to converge in the OR protocol. After learning was completed, it transmitted only approximately 10% of the packets through the wormhole tunnel, which was approximately half that under AODV. This was because, in OR, communication with the surrounding nodes was done to select the candidate nodes before packet transmission, enabling the exchange of information about the routing situation of the packets and malicious nodes. One of the key factors contributing to the improved performance of the proposed technique was the communication between neighboring nodes for selecting optimal candidate nodes before actually transmitting the packets. This exchange of

routing information and detection of potential malicious nodes played a vital role in enabling the proposed method to make informed decisions, effectively mitigating the impact of wormhole attacks.

To ensure the validity of the simulation results, we performed multiple runs, each incorporating different random node movements. The results consistently demonstrated the superiority of the proposed method compared with both the conventional and AIS-based routing protocols.

The ratio of the packets passing through the wormhole tunnel did not converge to zero under either the proposed method or the AIS wormhole detection method because of the nature of MANETs. Unlike traditional networks, MANETs do not have a centralized infrastructure or communication device; therefore, the detection of malicious nodes is solely based on the information exchange between nodes. Therefore, even if a malicious node is detected, this information is only transmitted via broadcasts, and the nodes that do not receive this signal remain unaware of the presence of the malicious node. Additionally, because the positions of the nodes change in real time, a node that enters the communication range of a malicious node without receiving the broadcast signal ends up sending packets to the malicious node according to the routing algorithm. In other words, due to the strict nature of the network structure, the packets sent to a wormhole tunnel cannot be completely blocked, even over time.

VI. CONCLUSION

This study introduces a Q-learning-based algorithm that incorporates a trust system for detecting wormhole attacks in Mobile Ad Hoc Networks (MANETs). Considering the characteristics of wormhole attacks, the proposed method dynamically adjusts the Q-value corresponding to the trust level of nodes when suspicion of a wormhole attack arises during routing. Amidst the validation process, nodes with Q-values falling below a specified threshold are identified as malicious, triggering their exclusion from the system to uphold stable routing. Crucially, this method is not limited to a particular routing algorithm and can be applied to both reactive (e.g., DSR and AODV) and opportunistic routing protocols. Hence, it is suitable not only for general MANETs but also for more sensitive wireless networks like underwater sensor networks and vehicular ad hoc networks.

Simulation experiments demonstrate that our proposed method can avoid wormhole tunnels more effectively than conventional routing-based wormhole detection methods and AISs. However, despite this success, the intrinsic features of MANETs, characterized by independent and real-time moving nodes with limited information transfer capabilities, pose practical challenges in simultaneously notifying all nodes of a detected malicious node. During our simulations, the proposed method was unable to limit the percentage of nodes passing through the tunnel to less than 10%. To overcome this limitation, our future efforts will focus on devising a mechanism to disseminate information about malicious nodes to a larger network segment more efficiently.

Some potential approaches to achieve broader dissemination of threat data and efficient propagation of information concerning detected malicious nodes include setting intermediate nodes as information relays and leveraging broadcast mechanisms or clustering techniques. By addressing this challenge, we aim to further enhance the effectiveness of the proposed method in securing MANETs against wormhole attacks.

REFERENCES

[1] P. Gupta, "A literature survey of MANET," *Int. Res. J. Eng. Technol.*, vol. 3, pp. 95–99, Feb. 2016.

[2] T. Jamal and S. A. Butt, "Malicious node analysis in MANETS," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 859–867, Dec. 2019, doi: 10.1007/s41870-018-0168-2.

[3] R. Maulik and N. Chaki, "A study on wormhole attacks in MANET," *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.*, vol. 3, pp. 271–279, Jan. 2011.

[4] J. Karlsson, L. S. Dooley, and G. Pulkkis, "A new MANET wormhole detection algorithm based on traversal time and hop count analysis," *Sensors*, vol. 11, no. 12, pp. 11122–11140, Nov. 2011, doi: 10.3390/s111211122.

[5] J. Ryu and S. Kim, "Reputation-based opportunistic routing protocol using Q-learning for MANET attacked by malicious nodes," *IEEE Access*, vol. 11, pp. 47701–47711, 2023, doi: 10.1109/ACCESS.2023.3242608.

[6] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)," *IEEE Access*, vol. 9, pp. 11872–11883, 2021, doi: 10.1109/ACCESS.2021.3051491.

[7] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. IEEE INFOCOM 26th IEEE Int. Conf. Comput. Commun.*, Anchorage, AK, USA, 2007, pp. 107–115, doi: 10.1109/INFCOM.2007.21.

[8] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 1998.

[9] S. Kim, *Game Theory Applications in Network Design*. Hershey, PA, USA: IGI Global, 2014.

[10] G. Yunchuan, H. Zhang, L. Zhang, L. Fang, and F. Li, "Incentive mechanism for cooperative intrusion detection: An evolutionary game approach," in *Proc. Int. Conf. Comput. Sci.*, vol. 10860. Cham, Switzerland: Springer, 2018, pp. 83–97, doi: 10.1007/978-3-319-93698-7_7.

[11] X. Liao, D. Hao, and K. Sakurai, "Classification on attacks in wireless ad hoc networks: A game theoretic view," in *Proc. 7th Int. Conf. Networked Comput. Adv. Inf. Manage.*, Gyeongju, (South) Korea, Jun. 2011, pp. 144–149.

[12] Z. Teng, C. Du, M. Li, H. Zhang, and W. Zhu, "A wormhole attack detection algorithm integrated with the node trust optimization model in WSNs," *IEEE Sensors J.*, vol. 22, no. 7, pp. 7361–7370, Apr. 2022, doi: 10.1109/JSEN.2022.3152841.

[13] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and wormhole attack detection model for RPL-based Internet of Things using machine learning," *Sensors*, vol. 22, no. 18, p. 6765, Sep. 2022, doi: 10.3390/s22186765.

[14] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*. Boston, MA, USA: Springer, 1996, pp. 153–181.

[15] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. WMCSA. 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, New Orleans, LA, USA, 1999, pp. 90–100, doi: 10.1109/MCSA.1999.749281.

[16] N. Chakchouk, "A survey on opportunistic routing in wireless communication networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2214–2241, 4th Quart., 2015, doi: 10.1109/COMST.2015.2411335.

[17] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

[18] H. Sun Chiu and K.-S. Lui, "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," in *Proc. 1st Int. Symp. Wireless Pervasive Comput.*, Phuket, Thailand, 2006, pp. 1–6, doi: 10.1109/ISWPC.2006.1613586.

[19] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," in *Proc. 1st ACM Workshop Secur. Ad Hoc Sensor Netw.*, Washington, DC, USA, Oct. 2003, pp. 21–32, doi: 10.1145/986858.986862.

[20] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2004, pp. 241–245.

[21] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Proc. Int. Conf. Dependable Syst. Netw.*, Yokohama, Japan, 2005, pp. 612–621, doi: 10.1109/DSN.2005.58.

[22] P. V. Tran, L. X. Hung, Y. K. Lee, S. Lee, and H. Lee, "TTM: An efficient mechanism to detect wormhole attacks in wireless ad-hoc networks," in *Proc. 4th IEEE Consumer Commun. Netw. Conf.*, Jan. 2007, pp. 593–598, doi: 10.1109/CCNC.2007.122.

[23] H. Chen, W. Lou, X. Sun, and Z. Wang, "A secure localization approach against wormhole attacks using distance consistency," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, pp. 1–11, Dec. 2009, doi: 10.1155/2010/627039.

[24] J. Biswas, A. Gupta, and D. Singh, "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol," in *Proc. 9th Int. Conf. Ind. Inf. Syst. (ICIIS)*, Gwalior, India, Dec. 2014, pp. 1–6, doi: 10.1109/ICIINFS.2014.7036535.

[25] S. Jamali and R. Fotohi, "Defending against wormhole attack in MANET using an artificial immune system," *New Rev. Inf. Netw.*, vol. 21, no. 2, pp. 79–100, Jul. 2016, doi: 10.1080/13614576.2016.1247741.

[26] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, vol. 2, Coimbatore, India, Apr. 2017, pp. 526–531, doi: 10.1109/ICECA.2017.8212719.

[27] M. Shukla, B. K. Joshi, and U. Singh, "Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET," *Wireless Pers. Commun.*, vol. 121, no. 1, pp. 503–526, Nov. 2021, doi: 10.1007/s11277-021-08647-1.

[28] D. Han, M. Liu, T.-H. Weng, C. Tang, M. D. Marino, and K.-C. Li, "A novel secure DV-hop localization algorithm against wormhole attacks," *Telecommun. Syst.*, vol. 80, no. 3, pp. 413–430, Jul. 2022, doi: 10.1007/s11235-022-00914-1.

[29] M. Abdan and S. A. H. Seno, "Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network (MANET)," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Jan. 2022, doi: 10.1155/2022/2375702.

[30] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu, and L. Chen, "CREDND: A novel secure neighbor discovery algorithm for wormhole attack," *IEEE Access*, vol. 7, pp. 18194–18205, 2019, doi: 10.1109/ACCESS.2019.2894637.

[31] O. R. Ahutu and H. El-Ocla, "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks," *IEEE Access*, vol. 8, pp. 63270–63282, 2020, doi: 10.1109/ACCESS.2020.2983438.

[32] K.-H. Chiang and N. Shenoy, "A 2-D random-walk mobility model for location-management studies in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 53, no. 2, pp. 413–424, Mar. 2004, doi: 10.1109/TVT.2004.823544.

[33] D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa, and R. H. Jhaveri, "A survey of reactive routing protocols in MANET," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Chennai, India, Feb. 2014, pp. 1–6, doi: 10.1109/ICICES.2014.7033833.

[34] V. Mahajan, M. Natu, and A. Sethi, "Analysis of wormhole intrusion attacks in MANETS," in *Proc. MILCOM - IEEE Mil. Commun. Conf.*, San Diego, CA, USA, Nov. 2008, pp. 1–7, doi: 10.1109/MILCOM.2008.4753176.

[35] M. Sadeghi and S. Yahya, "Analysis of wormhole attack on MANETs using different MANET routing protocols," in *Proc. 4th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Phuket, Thailand, Jul. 2012, pp. 301–305, doi: 10.1109/ICUFN.2012.6261716.

[36] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Proc. Comput. Sci.*, vol. 56, pp. 384–390, Jan. 2015, doi: 10.1016/j.procs.2015.07.224.

[37] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3224–3237, Dec. 2014, doi: 10.1109/TAC.2014.2351871.

[38] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Netw.*, vol. 13, no. 1, pp. 27–59, Feb. 2007, doi: 10.1007/s11276-006-3723-x.

[39] C. J. C. H. Watkins, "Learning from delayed rewards," Ph.D. dissertation, Dept. Comput. Sci., Univ. Cambridge, Cambridge, U.K., 1989.

[40] S. A. Bhosale and S. S. Sonavane, "Wormhole attack detection system for IoT network: A hybrid approach," *Wireless Pers. Commun.*, vol. 124, no. 2, pp. 1081–1108, May 2022, doi: 10.1007/s11277-021-09395-y.

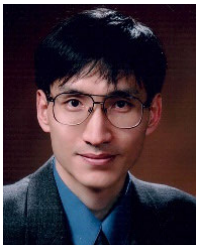
[41] Z. Zhao, B. Wei, X. Dong, L. Yao, and F. Gao, "Detecting wormhole attacks in wireless sensor networks with statistical analysis," in *Proc. WASE Int. Conf. Inf. Eng.*, 2010, pp. 251–254, doi: 10.1109/ICIE.2010.66.

[42] T. Giannetsos, T. Dimitriou, and N. R. Prasad, "State of the art on defenses against wormhole attacks in wireless sensor networks," in *Proc. 1st Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol.*, Aalborg, Denmark, May 2009, pp. 313–318, doi: 10.1109/WIRELESSVITAE.2009.5172466.

[43] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K.-Y. Lam, "Trust based routing for misbehavior detection in ad hoc networks," *J. Netw.*, vol. 5, no. 5, pp. 551–558, May 2010, doi: 10.4304/jnw.5.5.551-558.

[44] R. Feng, S. Che, X. Wang, and J. Wan, "An incentive mechanism based on game theory for trust management," *Secur. Commun. Netw.*, vol. 7, pp. 2318–2325, Dec. 2014, doi: 10.1002/sec.941.

JOONSU RYU (Graduate Student Member, IEEE) received the B.S. degree in mathematics and computer science from Sogang University, Seoul, Republic of Korea, in 2015, where he is currently pursuing the Ph.D. degree in computer science and engineering. His research interests include reinforcement learning, game theory, routing problems, and social networks.



SUNGWOOK KIM received the B.S. and M.S. degrees in computer science from Sogang University, Seoul, Republic of Korea, in 1993 and 1995, respectively, and the Ph.D. degree in computer science from Syracuse University, Syracuse, NY, USA, in 2003, under the supervision of Prof. Pramod K. Varshney. He was a Faculty Member with the Department of Computer Science, Chung-Ang University, Seoul. In 2006, he returned to Sogang University, where he is currently a Professor with the Department of Computer Science and Engineering and the Research Director of the Network Research Laboratory. His research interests include resource management, online algorithms, adaptive quality-of-service control, and game theory for network design.