International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212333 Volume 9, Issue 2, March – April (2022)

RESEARCH ARTICLE

Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT

Ga Hyeon An
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea
angachi576@skku.edu

Tae Ho Cho
Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
thcho@skku.edu

Received: 11 January 2022 / Revised: 23 February 2022 / Accepted: 01 March 2022 / Published: 30 April 2022

Abstract – The Internet of Things (IoT) is a technology that enables various IoT devices to collect data through sensors or sensor networks and to allow devices to share the collected data in an internet environment. Therefore, most communication is made wirelessly, and it is very vulnerable to a blackhole, selective forwarding, and sinkhole attacks that can occur in the network. One of the destructive attacks is the sinkhole attack, which compromises the integrity and reliability of data in a network. In general, the sinkhole attack detection method used by ad hoc networks and WSNs is less effective than the method used for IoT because of environmental differences. Therefore, the Intrusion detection of SiNkhole attack on 6LoWPAN for InterneT of Things (INTI) method can detect sinkhole attacks occurring in IoT. In this study, rules are defined using a specification-based approach of intrusion detection technology based on the number of input/output transmissions collected in the monitoring phase of INTI. Knowledge base rules were defined to thresholds of normal operation, and different rules were defined according to the role each node plays in improving sinkhole attack detection rates.

Index Terms – Wireless Sensor Network, Internet of Things, Sinkhole, Intrusion Detection, Artificial Intelligence, Rule Based System, Forward Chaining.

1. INTRODUCTION

1.1. Internet of Things and Attack

As shown in Figure 1, the Internet of things (IoT) collects data through sensors built into various IoT devices or wireless sensor networks that exist outside and communicate unattended through the internet without human intervention. It is also a technology that allows each IoT device to share the collected data [1]. The main goal of IoT is to connect things, such as sensors, computers, refrigerators, and automobiles, to the internet anytime, anywhere, and not just in everyday life [2]. However, with the widespread development of IoT, problems related to information protection and security have arisen and must be addressed [3, 4].

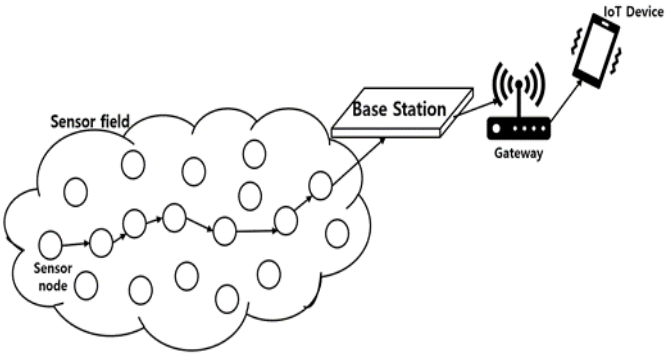

Figure 1 Internet of Things Based on WSN

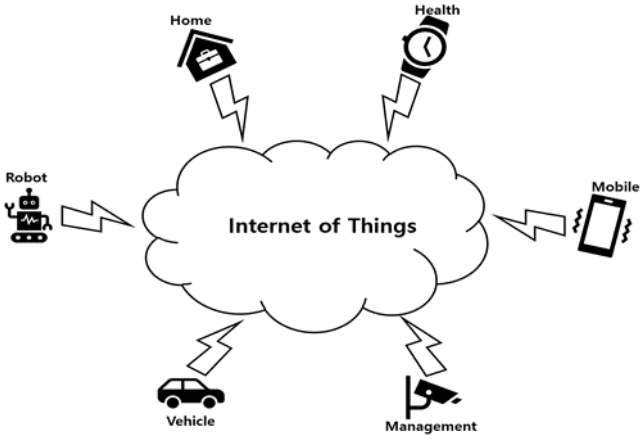

Figure 2 IoT Networks

Because most IoT communication is done wirelessly as shown in Figure 2, it is very vulnerable to attacks such as

RESEARCH ARTICLE

hello flood attacks, black hole attacks, sinkhole attacks, and spoofing as shown in Figure 3 [5]. Among them, the sinkhole attack is one of the destructive attacks that occur in the network and damage the integrity and reliability of data [6]. An attack is in which an attacker lures a packet through a malicious node to route the packet to the wrong path or drop the packet in the middle [3].

There are various existing sinkhole attack detection methods used in ad hoc networks or WSNs. However, these methods are not suitable for use in IoT in terms of security and energy [7]. Therefore, methods such as VeRA [8], SVELTE [9], SOS-RPL [10], and INTI [11] have been proposed to detect sinkhole attacks on the Internet of things.

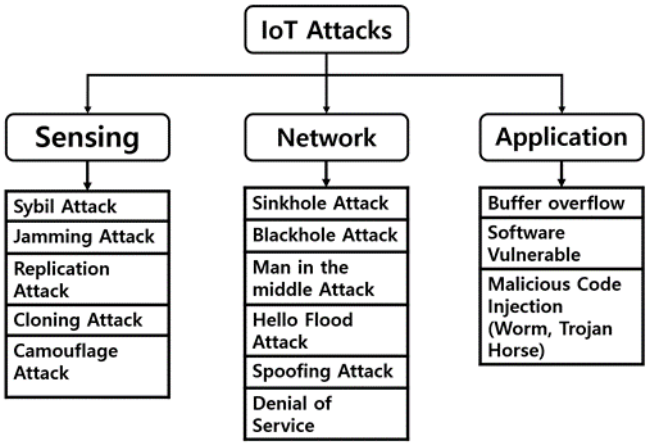

Figure 3 Attack by an IoT Layer

1.2. Research Objective

In this study, a technology that can defend against sinkhole attacks, which is one of the destructive attacks that can occur in IoT, was studied. As mentioned earlier, sinkhole attack detection methods commonly used in ad hoc networks and WSNs are difficult to use in IoT due to environmental differences. In this paper, in the attack detection process of Intrusion detection of SiNkhole attack on 6LoWPAN for InterneT of ThIngs (INTI) [11], which is one of the methods for detecting sinkhole attacks in IoT, the rules were defined using specification-based approaches of intrusion detection. Knowledge-based rules are defined differently for each node. Each rule is executed using a forward chaining inference engine. This method shows an improvement in the sinkhole attack detection rate.

1.3. Paper Outline

This paper flows in the following order: Section 2 discusses the sinkhole attacks, intrusion detection, INTI, and forward chaining. Section 3 describes the proposed modeling for detecting sinkhole attacks. Section 4 describes the experimental results of the proposed technique. Section 5 introduces further research. Finally, Section 6 writes the conclusion.

2. RELATED WORK

The IoT combines with the Internet, mobile networks, and intelligent devices to provide useful services to users. However, it has not yet been fully developed in terms of security, and it is unstable. The most important part of IoT security today is protecting personal data. Various attacks [7] can occur in networks, and it is important to detect attacks through a defense technique that can only be used in the IoT, besides the defense technique used in the ad hoc network or WSN.

2.1. Sinkhole Attack

In a sinkhole attack, as shown in Figure 4, an attacker starts an attack by compromising a node inside the network and turning it into a compromised node. Then, it creates sinkholes around the malicious node created by the attacker by enticing traffic through the malicious node [5].

A sinkhole attack works by making malicious nodes look attractive. For example, it can broadcast to neighboring nodes, which is the fastest route to send a packet using an attacking node [12].

As mentioned above, the sinkhole, in which a compromised node induces packets, is a destructive attack that damages the integrity and reliability of data by routing packets to the wrong path or dropping packets in the middle. Additionally, selective forwarding attacks can also occur through sinkhole attacks, and more serious attacks can occur when sinkhole attacks combine with other attacks [13].

Various methods were used to detect sinkholes in the IoT. SVELTE [7] uses a hybrid approach of signature and anomaly-based detection of intrusion detection to target attacks such as sinkholes, selective forwarding, spoofing, or altered routing information. It is a lightweight yet effective IoT intrusion detection system with an RPL routing protocol within the 6LoWPAN system [14].

VeRA [8] requires security precautions when updating the version number in the RPL, where a destination-oriented directed acyclic graph (DODAG) [2] route can initiate a reconfiguration of its routing topology [15]. Security precautions must also be taken to prevent the compromised DODAG nodes from publishing reduced rank values. This allows many parts of the DODAG to connect to the DODAG root through an attacker and many parts to eavesdrop. The way to have a malfunctioning node detected is based on the version number and rank value. INTI [11] consists of four phases: cluster configuration phase, monitoring node phase, attack detection phase, and attack isolation phase. It is an IDS for identifying sinkhole attacks and evaluating the behavior of

RESEARCH ARTICLE

each node. The details of the INTI are described in Section 2.2.

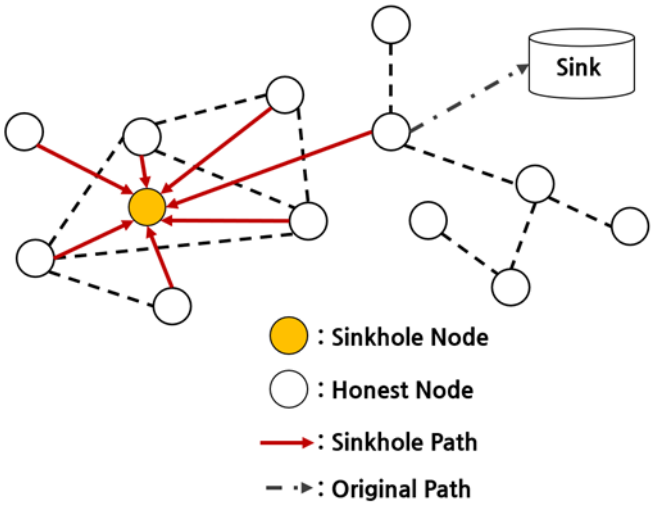

Figure 4 Sinkhole Attack

2.2. Intrusion Detection of SiNkhole Attack on 6LoWPAN for InterneT of ThIngs (INTI)

As described in Section 2.1, there are several defense techniques against sinkhole attacks that occur in the IoT. INTI is explained here.

As shown in Figure 5, INTI [11] consists of four stages: cluster configuration, monitoring node, attack detection, and attack isolation. The initial network consists of only free nodes. Initially, the clustering configuration stage and free nodes exchange control messages through message broadcasting to estimate the number of neighboring nodes. Based on the estimated number of neighbor nodes, the node with the largest number of neighbor nodes compared to other nodes is selected as the leader node, the free node receiving the message from the leader node becomes the member node, and two or more leader nodes among the member nodes designate the node that receives the message as the related node. A cluster consists of a leader node, member nodes, and related nodes. Member nodes are responsible for detecting events that occur within a cluster and delivering messages to the leader node. The leader node is responsible for delivering the message received from the member node to the related node. A related node is a node that receives messages from two leader nodes and plays a role in delivering the message received from one leader node and information on the cluster in which the node exists to the other leader node. The network configuration of INTI is shown in Figure 6. In the second stage, the monitoring node stage defines a monitoring module that counts the number of I/O transmissions performed by the node in charge of message delivery. In the third stage, the attack detection stage, the number of monitored input/output transmissions are defined using the β (α, β) distribution to define reputation and confidence, and through this, a sinkhole attack is detected. In the final attack isolation stage, all nodes are notified of the detected sinkhole, and the cluster is reconfigured after isolating the sinkhole node.

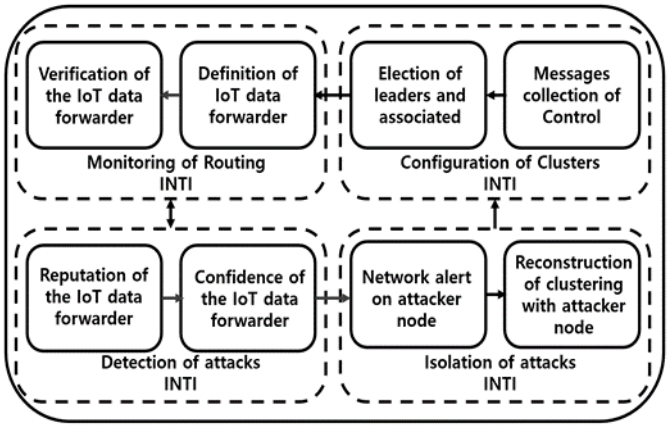

Figure 5 The INTI System Architecture

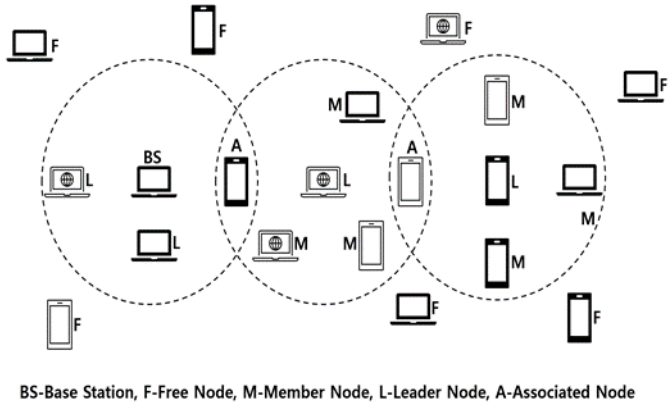

Figure 6 The INTI Network

2.3. Intrusion Detection

Intrusion is caused by a user who does not have access to a network system, a user who attempts to gain additional privileges besides the access privilege, or a user who misuses these access privileges. Such intrusions are accepted as attempts to compromise or circumvent the availability, confidentiality, or integrity of network security mechanisms [16], which detect and monitor events that occur inside a network or computer system and to identify security breaches by tracing abnormal systems usage patterns.

Intrusion detection technology can be classified into four types: specification, anomaly, signature, and hybrid approach according to the detection technology used in the network or system [17].

- The Signature-Based Approach

RESEARCH ARTICLE

The signature-based approach detects attacks when events originating inside networks and computer systems match the attack signatures stored in internal storage systems. An alert is triggered when an event matches a pattern/signature stored in an internal database.

The signature-based approach is highly accurate and effective in detecting attacks that our internal database knows in advance. However, it is not effective in detecting recent attacks that are modified from existing or unknown attacks [16].

- The Anomaly-Based Approach

The anomaly-based approach immediately compares the original behavior with the behavior that occurs inside the system and raises a warning alarm when deviations from existing behavior exceed certain thresholds. Unlike signature-based methods, this method is effective in detecting recent attacks that are unknown or unmodified in existing attacks.

However, it is very difficult to set a threshold for normal behavior because any inconsistency with normal behavior is recognized as an attack. Additionally, this method has a very high false-positive rate, which recognizes non-attack behaviors as attacks [18].

- The Specification-Based approach

The specification-based approach is a way in which users or experts define rules based on thresholds and expected behaviors from network components (protocols, routing tables, nodes, etc.) [15]. This method detects attacks when the behavior inside a network deviate from a set of user-defined thresholds and rules created.

This approach serves the same purpose as the anomaly-based approach discussed above to identify differences from the original behavior. However, unlike the anomaly-based approach, this method requires an expert or user to manually define each rule and threshold. As a result, it generally provides a lower false-positive rate than an anomaly-based approach [19]. However, manually defined rules and thresholds may not apply to other environments and are error-prone [18].

2.4. Forward Chaining

The expert system, which has been extensively used in artificial intelligence and is a system that allows the decision-making ability of an expert to be utilized in a computer. The expert system can be broadly divided into two systems: a knowledge base and an inference engine [20, 21]. The knowledge-based represents facts and rules, and rules connect logical information; it has an If... Then structure [22]. An inference engine is a method of applying existing or new facts to a rule so that new facts can be inferred from the rule. In addition to the knowledge base and inference engine, there is working memory. Working memory contains facts (information) provided by the user and the facts inferred by an inference engine.

Among the various inference engines, forward chaining is a method to draw a reasonable conclusion using the facts (information) given in the rule consisting of If...Then, or to establish additional hypotheses to infer the conclusion when additional facts (information) are drawn. That is, the facts (information) that exist in the working memory are If… Then, refers to the process of inferring a new fact by applying a rule consisting of it and storing it in the working memory or inferring a conclusion [23].

Forward chaining is illustrated in Figures 7 and 8, which illustrate the simple rules.

Rule 1.		Rule 5.	
If	The fever is above 37 degrees	If	Have a fever
then	Have a fever		Lose one's sense of smell
		then	COVID-19 confirmed
Rule 2.			
If	Your body feel cold	Rule 6.	
then	Have a fever	If	Have a cough
			Have a headache
Rule 3.		then	COVID-19 confirmed
If	Your throat hurt		
then	Have a cough	Rule 7.	
		If	Have a cough
Rule 4.			Got a sick
If	Have a fever	then	COVID-19 confirmed
	Have a cough		
then	COVID-19 confirmed		

Figure 7 Example of Forward Chaining Rule

As part of working memory, there is the fact that "The fever is above 37 degrees, one loses their sense of smell. "The condition of rule 1 matches the fact that "The fever is above 37 degrees" in working memory. So, rule 1 fire and an additional fact of "Have a fever" is inferred. If so, the new facts are updated in the working memory. The new fact "Have a fever" updated in working memory matches the conditions of Rules 4 and 5. In this situation, a rule is triggered. If more than one rule is triggered in this way, conflict resolution is used to resolve it, and specificity ordering is used to resolve it. The conflict resolution is discussed in the following. rule 5, which is conditional on the fact that "Have a fever and lose one's sense of smell" exists in the working memory, is fired, and it is possible to infer the conclusion that "COVID-19 confirmed" Figure 7 shows a pictorial representation of what is described above.

Conflict resolution is a conflict resolution strategy for deciding which rules to fire because you only want to fire one rule when over one rule is triggered. Below is a description of the various conflict resolutions [23, 24].

- Rule Ordering: Fires the rule with the higher priority of the triggered rule by sorting all the rules into a priority list.

RESEARCH ARTICLE

- Context Limiting: Reduces the likelihood of collisions by breaking rules into groups, only some of which are active at any time.
- Specificity Ordering: Among the triggered rules, the rule that satisfies the most conditions of the rule is fired first.
- Recency Ordering: Fires the most recently used rule.

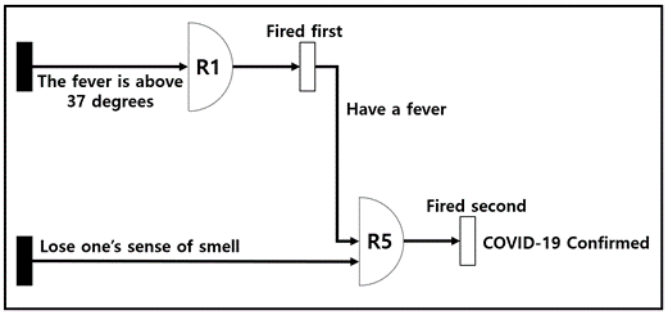

Figure 8 Forward Chaining

3. PORPOSED MODELLING

In this section, the simulation environment of the proposed technique and the proposed technique are explained with figures.

3.1. Problem Statement

As mentioned above, a sinkhole attack is one of the destructive attacks that compromise the reliability and integrity of data, and an attacker can compromise a node inside the network and lure the packet through this node to route the packet to the wrong path or drop the packet in the middle. This is an attack that makes it happen. IoT is vulnerable to attacks such as sinkholes because data collected through sensors or sensor networks are communicated and shared unattended. Therefore, a defense technique that can detect sinkhole attacks is required. Additionally, using a specification-based approach to define rules or thresholds can reduce false-positive rates. With the existing INTI method for detecting sinkhole attacks, the number of input/output transmissions calculated in the monitoring node stage was used for the β (α, β) distribution to define the reputation and confidence, and through this, a sinkhole attack was detected. We use the specification-based approach of intrusion detection in this study for defining thresholds and deviations in the attack detection stage, and we propose a technique for detecting sinkhole attacks by using the forward chaining inference engine of the expert system.

3.2. Environment Assumptions

The environmental assumptions of the proposed technique are as follows.

1. Monitoring node uses associated nodes existing in each cluster.
2. When forwarding a message, a node uses the shortest path routing.
3. When a member node detects an event, it sends a count to the monitoring node.
4. Whenever the leader node receives a message, it sends a count to the monitoring node.
5. Attacks do not occur simultaneously in multiple types of nodes.

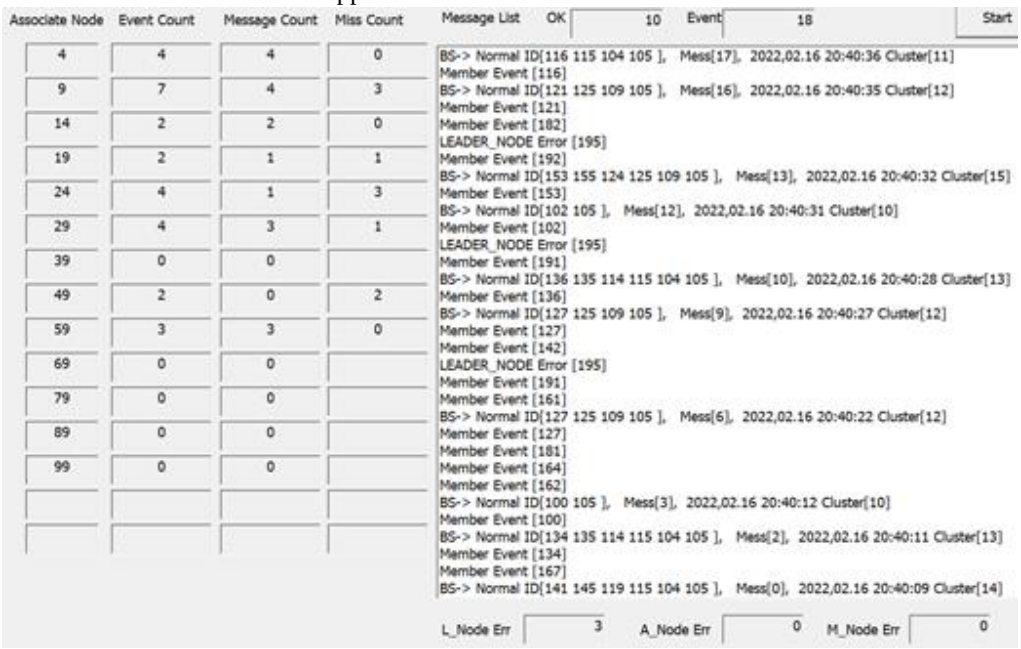

Figure 9 Proposed Technique Simulation

RESEARCH ARTICLE

Simulation Parameters	Explanation
Associate Node	Node ID number of the Associate node
Event Count	Number of detected events occurring in the Associate node scope
Message Count	The number of messages sent by detecting an event that occurred
Miss Count	A count representing the difference between the message count and the event count to detect a sinkhole attack that does not send a message by detecting an event that has occurred
OK	Number of messages successfully delivered to BS
Event	Number of events
L_Node Err	Number of cases where sinkhole attacks were detected by the leader node
A_Node Err	Number of cases where sinkhole attacks were detected by the associate node
M_Node Err	Number of cases where sinkhole attacks were detected by the member node
BS->Normal ID[ ], Mess[ ], Cluster[ ]	BS->Normal: Message arrived at BS, ID[ ]: Node ID of movement path, Mess[ ]: Message number that occurred, Cluster[ ]: Cluster number where event occurred
Member Event[ ]	Node number that detected the event that occurred
LEADER_NODE Error[ ]	In the case of a leader node when a sinkhole attack is detected during message delivery (leader node [number])
ASSOCIATE_NODE Error[ ]	In case of an associate node when a sinkhole attack is detected during message delivery (associate node [number])
MEMBER_NODE Error[ ]	A member node when a sinkhole attack is detected during message delivery (member node [number])

Figure 10 Simulation Parameter

Figure 9 shows the proposed technique simulation and Figure 10 represents the various simulation parameters used.

3.3. Proposed Technique

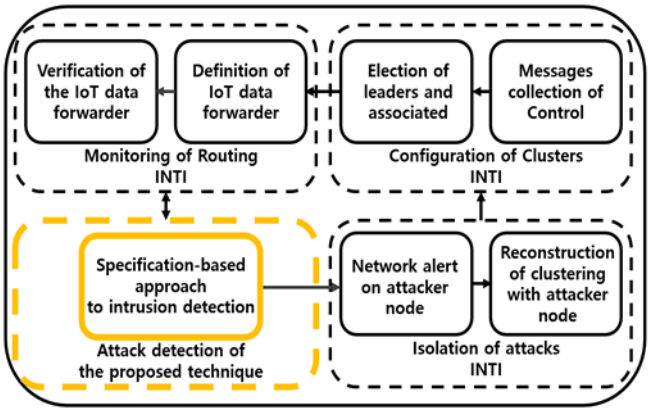

Figure 11 Proposed Technique Architecture

In this study, the proposed method for detecting a sinkhole attack is constructed in the attack detection stage, which is the third stage of INTI, as shown in Figure 11. After selecting a monitoring node in the monitoring node stage, which is the second stage of INTI, the monitoring node counts the number of messages input/output of member nodes and leader nodes existing in the cluster. Subsequently, in the attack detection stage, the threshold value and deviation are defined as rules of the knowledge base using the specification-based approach of intrusion detection. The roles of the associated node, member node, and leader node in the cluster are different, and a sinkhole attack may occur for each node. Therefore, when defining a rule as a knowledge base using the specification-based approach of intrusion detection, it should be applied differently to each node.

The application of the rule is: First, we need to define a threshold value for normal operation in which a node normally delivers a message in the network. Second, the threshold and deviation of the node's normal operation in the network are defined as the rule of the knowledge base through the number of I/O transmissions of the monitored message. Because it is a rule of the knowledge base, it is defined using the If…Then structure. Finally, the defined rule is executed

RESEARCH ARTICLE

using forward chaining, which is an inference engine of the expert system. There may be cases where two or more rules are triggered depending on the condition, and a conflict may occur. To resolve this situation, a conflict resolution method, the specificity rule ordering method, is used to resolve the conflict. The normal path of message transmission is shown in Figure 12.

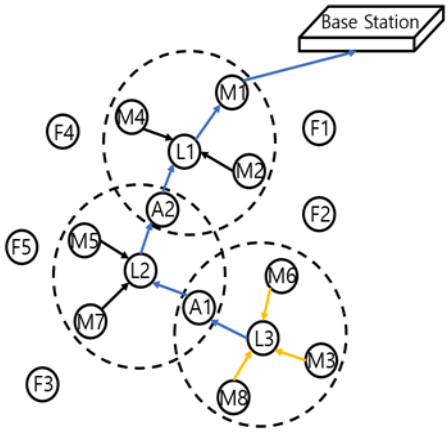

Figure 12 The Normal Path of Message Transmission

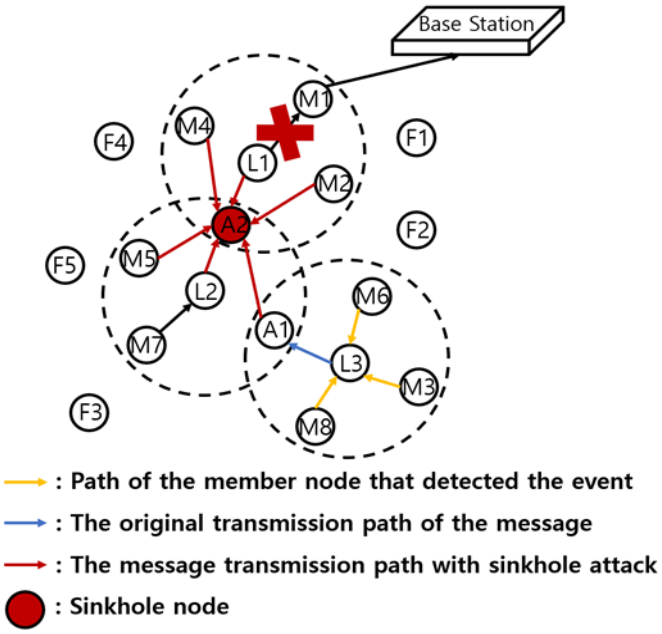

Figure 13 Message Transmission Path with Sinkhole Node

Associated nodes have an event count that increases when a member node detects an event within the cluster and a message count that increases when a node delivers a message. As shown in Figure 13, if a sinkhole attack has occurred in A2, the difference between the number of event counts and message count is four or more, and if node id is the associated node, the sinkhole has occurred in the associated node. Additionally, if it is assumed that a sinkhole attack has occurred in M2, the message count increases; if the node id is a member node, a sinkhole has occurred in the member node. Thus, different rules were applied to each node.

4. RESULTS AND DISCUSSIONS

The simulation environment was as follows: events occurred randomly, there were 100 nodes inside the sensor network, and there was a total of 10 clusters.

4.1. Proposed Technique Result

This is the result of detecting a sinkhole attack according to the number of events of 100, 200, and 300 in the simulation environment.

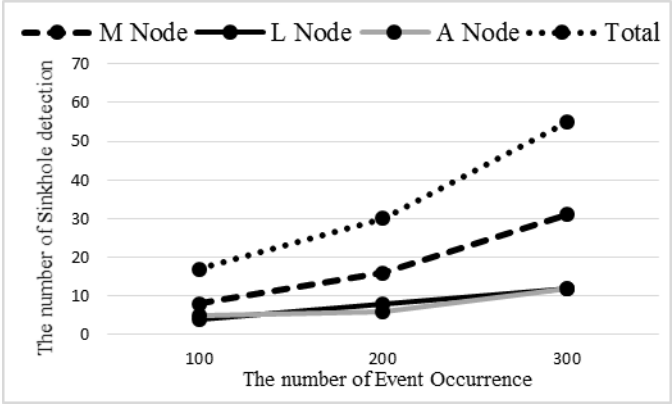

Figure 14 The Number of Sinkhole Attack Detections per Node According to the Number of Event Occurrences in the Existing Technique

In Figure 14, node M is a member node, node L is a leader node, and node A is a related node. Figure A shows that the sinkhole was detected in the order of member node, leader node, and related node, respectively, according to the number of sinkhole attack detections per node according to the number of event occurrences in the existing technique.

In Figure 15, node M is a member node, node L is a leader node, and node A is a related node. In Figure 14 showing the sinkhole detection of the proposed technique, similar to the result of Figure A, the number of sinkhole detections according to the number of events was detected well in the order of member nodes, leader nodes, and related nodes. As a result, the number of sinkhole attacks is inevitably large because the number of member nodes is the largest among the nodes in each cluster. Therefore, Figure 16 shows the sinkhole attack detection ratio for each node according to the attack ratio for accurate results.

RESEARCH ARTICLE

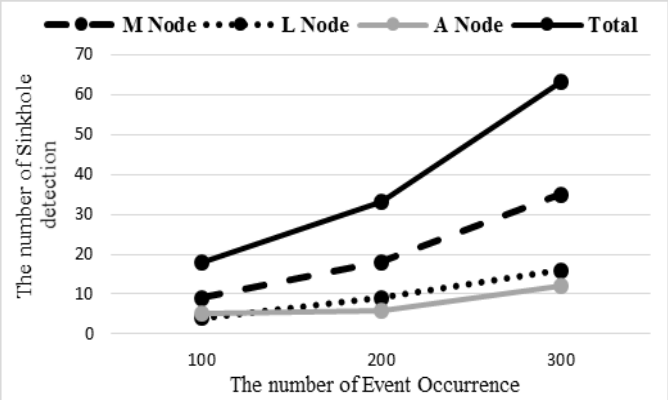

Figure 15 The Number of Sinkhole Attack Detections per Node in the Proposed Technique According to the Number of Event Occurrences

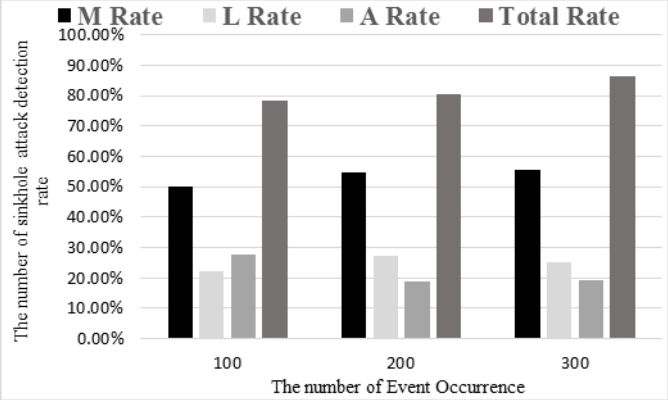

Figure 16 The Sinkhole Attack Detection Ratio Detected by Each Node by the Number of Event Occurrences

In Figure 16, M rate represents the sinkhole attack detection ratio detected by the member node, L rate represents the sinkhole attack detection ratio detected by the leader node, and A rate is the sinkhole attack detection ratio detected by the associated node. As shown in Figure 16, according to the number of events from 100 to 300, sinkhole attacks detected by member nodes for each node on average 53.3%, sinkhole attacks detected by leader node on average 24.9%, and sinkhole attacks detected by associated nodes. The average sinkhole attack ratio is 21.9%. In addition, the average detection ratio of sinkhole attacks for all nodes were 81.6%.

Figure 15 shows the number of sinkhole attack detections for each node according to the number of events from 100 to 300, and Figure 15 shows the sinkhole attack detection ratio for each node according to the number of events from 100 to 300.

Because both figures show the detection rate of each node in the sinkhole attack that occurred in the network, it is unknown which node the knowledge base rule using the expert system was applied well.

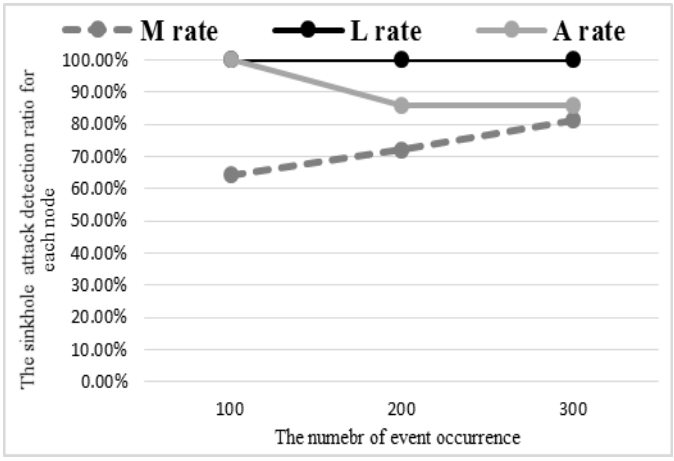

Figure 17 The Sinkhole Attack Detection Ratio for Each Node According to the Number of Events Occurrences

As shown in Figure 17, according to the number of event occurrences from 100 to 300, the sinkhole attacks detected by the member node for each node are 72.5% on average, and the sinkhole attacks detected by the leader node are, on average, 100% detected by the associated node. The average sinkhole attack ratio is 90.4%. As a result, because the leader node detects all sinkhole attacks, the knowledge-based rule using the expert system is applied well. In addition, the rule is being applied well because the ratio of detecting sinkhole attacks in member nodes also increases. However, in the case of the associated node, the detection ratio at 200 and 300 decreased compared to 100, but the ratio was maintained at 200 and 300.

4.2. Proposed Technique and INTI

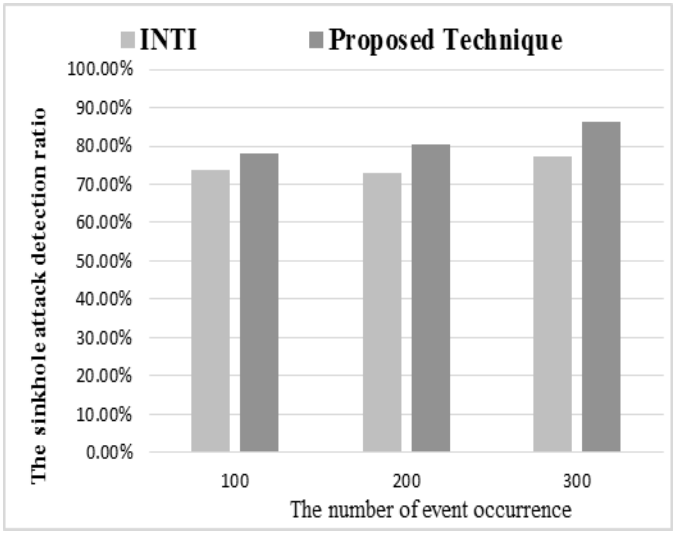

Figure 18 The Sinkhole Attack Detection Ratio Detected by the Proposed Technique and INTI According to the Number of Event Occurrences

RESEARCH ARTICLE

This is a comparison of the sinkhole attack detection ratio results in the proposed technique and the existing technique INTI, according to the number of events of 100, 200, and 300 in the same simulation environment.

As shown in Figure 18, according to the number of event occurrences from 100 to 300, the existing method, INTI, showed an average sinkhole attack detection ratio of 74.8%, and the proposed method showed an average sinkhole attack detection ratio of 81.63%. The proposed method showed an average sinkhole attack detection ratio of approximately 7% higher than that of the existing method, and the proposed technique escalates the sinkhole attack detection ratio as the number of events increases.

5. CONCLUSION

In this study, using a specification-based approach of intrusion detection, we define thresholds and deviations as rules of the knowledge base, and propose a technique to detect sinkhole attacks using a forward chaining inference engine. The proposed method improved the sinkhole attack detection ratio by approximately 7% on average compared with the existing method. However, when looking at the sinkhole detection ratio for each node of the proposed method, the knowledge-based rules were well applied in the member nodes and leader nodes but relatively less applied in associated nodes. If the rule was developed using the specification-based approach of intrusion detection, it may not be applied to an environment different from the existing one if it was developed in a different environment. Therefore, we plan to supplement the rules so that the proposed technique can be applied in various environments. Also, as mentioned above, a sinkhole attack is difficult to detect as it is a destructive attack that damages the reliability and integrity of data. The proposed method is based on the specification-based intrusion detection approach and creates rules based on the knowledge base of the expert system so that only sinkhole attacks can be detected. In future research, we plan to write additional rules to detect even selective forwarding attacks, which are one of the most common attacks through sinkhole attacks.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1A2C2005480).

REFERENCES

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805

[2] Hassan, Basma Mostafa. Monitoring the Internet of Things (IoT) Networks. Diss. Université Montpellier; Ğāmi'at al-Qāhirah, 2019.

[3] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[4] Mendez, Diego M., Ioannis Papapanagiotou, and Baijian Yang. "Internet of things: Survey on security and privacy." arXiv preprint arXiv:1707.01879 (2017).

[5] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

[6] Choudhary, Sarika and Nishtha Kesswani. "A Survey: Intrusion Detection Techniques for Internet of Things." IJISP vol.13, no.1 2019: pp.86-105. http://doi.org/10.4018/IJISP.2019010107

[7] Ahmed, Hassan I., et al. "A survey of IoT security threats and defenses." International Journal of Advanced Computer Research 9.45 (2019): 325-350.

[8] Dvir, Amit, and Levente Buttyan. "VeRA-version number and rank authentication in RPL." 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. IEEE, 2011.

[9] Raza, Shahid, Linus Wallgren, and Thiemo Voigt. "SVELTE: Real-time intrusion detection in the Internet of Things." Ad hoc networks 11.8 (2013): 2661-2674.

[10] Zaminkar, Mina, and Reza Fotohi. "SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism." arXiv preprint arXiv:2005.09140 (2020).

[11] Cervantes, Christian, et al. "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things." 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, 2015.

[12] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1.2-3 (2003): 293-315.

[13] Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing attacks and countermeasures in the RPL-based internet of things." International Journal of Distributed Sensor Networks 9.8 (2013): 794326.

[14] Chawla, Shiven. Deep learning based intrusion detection system for the Internet of Things. University of Washington, 2017.

[15] S., Gayathri K. and Tony Thomas. "Intrusion Detection Systems for Internet of Things." Handbook of Research on Intrusion Detection Systems, edited by Brij B. Gupta and Srivathsan Srinivasagopalan, IGI Global, 2020, pp. 148-171. http://doi:10.4018/978-1-7998-2242-4.ch008

[16] Bace, Rebecca Gurley, and Peter Mell. "Intrusion detection systems." (2001): 201.

[17] Smys, S., Abul Basar, and Haoxiang Wang. "Hybrid intrusion detection system for internet of things (IoT)." Journal of ISMAC 2.04 (2020): 190-199.

[18] Zarpelão, Bruno Bogaz, et al. "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84 (2017): 25-37.

[19] Faraj, Omair, et al. "Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things." Proceedings of the 15th International Conference on Availability, Reliability, and Security. 2020.

[20] Al-Ajlan, Ajlan. "The comparison between forward and backward chaining." International Journal of Machine Learning and Computing 5.2 (2015): 106.

[21] Mzori, Bareen Haval Sadiq. Forward and Backward Chaining Techniques of Reasoning in Rule-Based Systems. MS thesis. Eastern Mediterranean University (EMU)-Doğu Akdeniz Üniversitesi (DAÜ), 2015.

[22] Lodder, Arno R., and John Zeleznikow. "Artificial intelligence and online dispute resolution." Online Dispute Resolution: Theory and Practice A Treatise on Technology and Dispute Resolution (2012): 73-94.

[23] Winston, Patrick Henry, and Richard Henry Brown. "Artificial intelligence: an MIT perspective." Cambridge, Mass (1979): 1.

[24] B. George and S. S. Mathai, "Improving quality of interference in multilevel secure knowledge-based systems," 2004 International Conference on Machine Learning and Applications, 2004. Proceedings., 2004, pp. 477-484, doi: 10.1109/ICMLA.2004.1383553.

RESEARCH ARTICLE

Authors

Ga Hyeon An received her B.S degree in the Department of Electronic Communication Engineering from Dealim University, in February 2021. Her research interests include wireless sensor network, IoT, machine learning and deep learning.

Tae Ho Cho received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.

How to cite this article:

Ga Hyeon An, Tae Ho Cho, "Improving Sinkhole Attack Detection Rate through Knowledge-Based Specification Rule for a Sinkhole Attack Intrusion Detection Technique of IoT", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 169-178, 2022, DOI: 10.22247/ijcna/2022/212333.