Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 01, January-2021

Detecting a False Report using Temporal Logic and a Rank Algorithm in WSNs

Jungsub Ahn
Department of Electrical and Computer Engineering,
Sungkyunkwan University
Suwon, Republic of Korea

Taeho Cho*
Department of Computer Science and Engineering,
Sungkyunkwan University
Suwon, Republic of Korea

Sanghyeok Lim
Amorepacific
Seoul, Republic of Korea

***Abstract*— Wireless sensor networks (WSNs) self-organize clusters via communication between multiple sensor nodes that are deployed across a large field and an open environment. Therefore, nodes can be easily compromised, and attackers can launch false report injection attacks through compromised nodes. Several security protocols based on a message authentication code (MAC), such as the Probability Voting based Filtering Scheme, have been proposed to prevent application-layer attacks. MAC-based protocols remain vulnerable to high-level attacks where all MACs have false event values. We propose a temporal logic-based security model that allows the base station to defend against false report attacks by executing report authenticity detection using a temporal logic rule.**

Keywords—False Report Detection; Temporal Logic based Inference; Wireless Sensor Networks Security; Intelligence False Report Injection Attack;

I. INTRODUCTION

Wireless sensor networks (WSNs) are used for gathering information in various scenarios, such as war, disaster, and home network systems, using sensor nodes deployed in the field. Sensor nodes have restricted performance to extend the lifetime of the network. In particular, sensor nodes are scattered in an open environment and can be easily compromised by an adversary. These vulnerabilities allow network attackers to launch false report injection attacks or other types of attacks that insert the wrong MAC into the report. These attacks inject events that have not actually occurred, causing unnecessary energy consumption of nodes or false alarms to the network manager. Several security protocols have been proposed to prevent such attacks [1-4]. These security protocols perform report verification based on common message authentication codes (MACs), and manage security and energy efficiency by discarding reports when the report is falsely determined through report verification performed by the node. The security protocol checks the integrity of the report at the BS. If all of the MACs in the report are not compromised, normal filtering is possible and false alarms are avoided. However, if all key values included in the false report are stolen and have normal MACs, the secondary verification at the BS is invalid and can cause problems such as false alarms and inappropriate response to events.

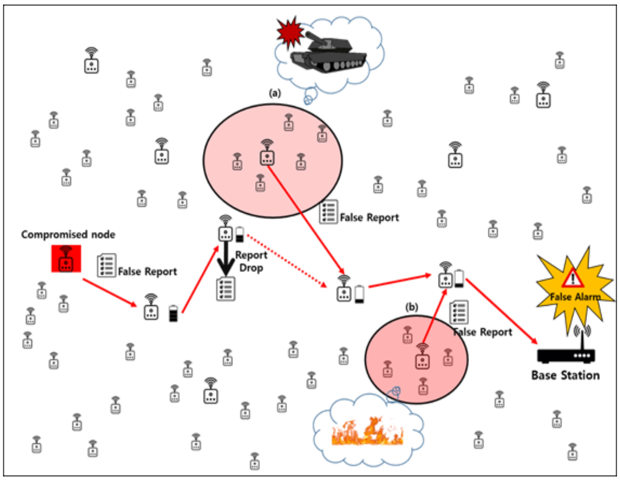


Fig. 1. False report injection attack scenario

The proposed MAC-based security protocols used to filter false reports cannot provide security for full MAC reliability [1]. Additionally, widespread node damaged situations have stated that they will launch attacks other than false report injection attacks from the application layer, which indicates that a full MAC hijacking attack can occur, and there is a need for a solution. We present a security model for false report attacks using the statistical model based on temporal logic (TL) as a secondary verification applied to the situation that cannot be verified by the existing MAC-based security protocol in this paper. A false report security based on a statistical model using TL is used to build a virtual simulation environment similar to WSN and store statistics about the state values of each event in the database and express only a normal state transition. TL is a model used to determine whether the status of nodes is normal or abnormal by applying statistics and ranking of rules and state variation. The introduction of a statistics-based ranking algorithm for state variation is used to improve the detection accuracy of intelligent attacks and the false-positive rate for normal nodes.

The performance evaluation of the model was based on the assumption of fire in the WSN field. In addition, the simulation was modeled by a cellular automata (CA) based fire transition, and the simulation was conducted considering variables such as the initial fire occurrence point, wind speed, wind direction, and fire transition probability. The proposed model was designed to determine the state of the node (either normal or attacked) by setting the detection threshold and comparing the number and ratio of abnormal state transitions with the threshold. Using experiments with the proposed model, the nodes sending false information considering the location of the initial fire and the influence of the wind were tracked. In addition, we compared the proposed model with the Probability Voting based Filtering Scheme (PVFS), a cluster-based security protocol, to analyze the performance.

This paper is organized as follows. Section 2 describes the limitations of MAC-based security protocols and en-route filtering, PVFS and TL, which are the basis of the proposed scheme. Section 3 details the statistical period ranking algorithm using TL used in the proposed scheme. Section 4 discusses the results of the experiment, and Section 5 discusses conclusions and future work.

II. BACKGROUNDS

A. *En-route filtering*

En-route filtering verifies the report that the intermediate nodes are between the source and sink. En-route filtering prevents the unnecessary energy consumption of transmission by early removal of false reports through MACs. Nodes store a key set to generate a MAC. When a node detects an event, it generates a MAC using the distributed key and hash function that includes the MAC in the generated report. Various schemes have been proposed for the key distribution method. MAC is verified using a symmetric key between nodes. Encrypted MAC content depends on detailed event information in a report and the key distributed. A intermediate node generates and compares a MAC to certify the legality of the report. If a MAC is normal, the report is transmitted to the upper node. If the MAC is different, the report is considered false and the report is removed. En-route filtering prevents the WSN from interfering with missions such as false report injection attacks [5,6], DoS attacks [7], selective forwarding attacks [8], and report disruption attacks [9].

B. *MAC-based security protocol requirements*

The MAC-based security protocol performs the final inspection at the base station (BS). However, if nodes are as compromised as the security threshold, the attacker can create a completely false report that cannot be filtered by the BS and en-route. Solving these problems is important because it causes incorrect behavior in report-dependent control systems. As a result, there needs to be a way to recognize the state of a node and provide security for it. We proposed a context-based security provision method based on the report contents that considers all MACs damaged in the reports MAC-based security protocol. In our scenario, TL is used to provide security enhancement using an inference algorithm that traces the location of compromised nodes from the time of attack detection through the fire prediction model. The TL-based primary detection for detecting abnormal behavior patterns is performed, and a probability-based secondary detection for detecting an intelligent attack is performed.

C. *Probability voting based filtering scheme*

In WSN, false report injection attacks occur to deplete sensor node energy and generate false alarms in the BS. The attacker also performs a false MAC injection attack to prevent reaching the BS of the report containing normal event information. PVFS has been proposed to prevent these two types of attacks from the application layer. PVFS is a cluster-based security protocol. Fig. 2 shows the report generation and filtering in PVFS.

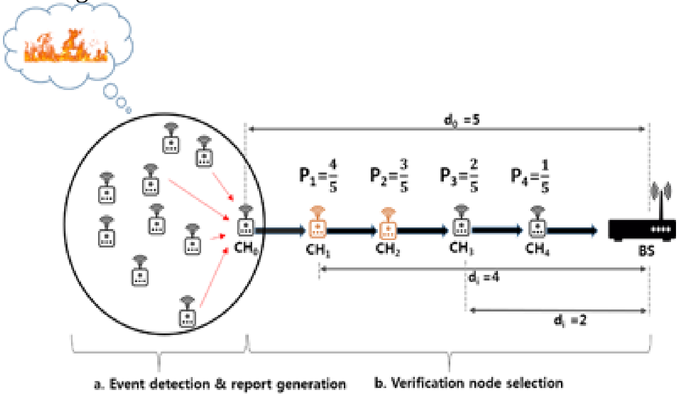


Fig. 2. Probability voting based filtering scheme

When the cluster head (CH) node detects an event, it generates a report in collaboration with neighbor sensor nodes in the cluster. The report contains the MAC encrypted with the security key of the node participating in the report generation.

PVFS elects a report verification node among CH nodes to prove the authenticity of the report. Fig. 3 shows the selection and filtering process of the verification node. The event detection node cannot transmit the report directly to the BS. Therefore, the CH node forwards the report to the BS via hop-by-hop communication between the CH nodes. Among the various CHs, the node that is responsible for verifying the report is selected with probability based on the number of hops between the BS and event detection node. The Px in Fig. 2 indicates the probability that each node will be selected as a report verification node. In general, the closer to the event detection cluster, the higher the probability of being selected as a verification node. CH nodes selected as verification nodes are randomly given keys of member nodes of the event detection cluster, and when the report arrives, the authenticity of the report is determined by comparing the key index and MAC value.

PVFS and many other cluster-based security protocols offer a high level of security through an en-route filtering detection method. However, if nodes greater than the security threshold are compromised, then the report includes MAC values that cannot be filtered. This is a vulnerability of all MAC-based application layer protocols including PVFS. In addition, when a large number of a nodes are compromised by attacks, the network manager does not have any countermeasures in the existing security method. Therefore, a new security method that does not depend on MACs is needed to prevent this situation.

D. *Spatio-temporal logic*

Temporal logic (TL) is a useful logical system that simultaneously represents the concept of time and space. TL can express the dynamic behavior of a reactive program in a real-time system and is widely used in systems intended to run indefinitely [10, 11]. TL detects elements that change over time and makes complex inferences. It is possible to infer new relational knowledge in a complex system because the system can use embodied expressions about the event as the concept of time expands, rather than logic treated only with existing events, conditions, and spatial concepts. The proposed scheme was focused on determining the wrong behavior in the network security system. The application of TL in the network security system has the advantage of being able to detect new attacks that cannot be discovered by existing methods using time and space values rather than the symmetric–key algorithm based authentication method through spatio–temporal knowledge inference.

TL uses temporal and spatial operators and various symbols to express logic. TL often contains operators such as ‘O’, meaning in the next moment in time, ‘□’ meaning at every future moment, and ‘◇’ meaning at some future moment [12].

III. PROPOSED SCHEME

We performed a simulation based on CA-based fire prediction model for statistical data collection for probability-based detection algorithm. The motivation of the proposed scheme is described in Section 3.1. Section 3.2 describes the CA-based fire prediction learning model. Section 3.3 describes in detail the CA-based statistical ranking algorithm for a secondary defense method.

A. Motivation

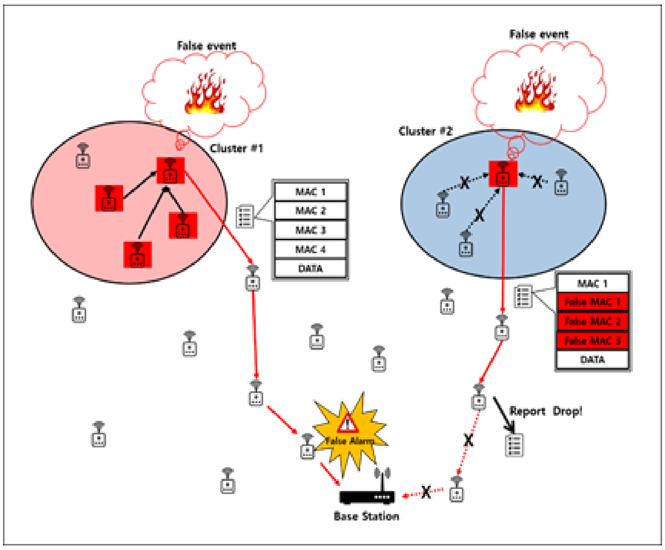


Fig. 3. Various attacks in the WSN field

Security protocols, such as PVFS [1], DEF [4], SEF [13], and CCEF [3], have been proposed to detect false reports in the application layer of WSN. A sensor node that detects an event creates a report on the sensing event information and attached MACs to block the illegal report from the compromised nodes in application layer security protocols.

If all MACs of the report created by the compromised node are false data or all of the key information that constitutes it is exposed, the intermediate nodes judge the report containing false event information as normal. Moreover, proper verification is not performed at the BS. As a result, a false alarm occurs or an incorrect corrective action is executed in the BS, which is a weakness of several security protocols. The MAC-based security protocol should not depend on the MAC for security for a large number of node hijack attacks, instead recognizing the monitoring status of the entire field, and additional verification must be performed at the BS.

To solve this problem, a genetic algorithm based fuzzy logic optimization method (FLOM) [14] and context-aware architecture (CAA) [15] that recognizes the situation of the field and performs security was proposed. However, this scheme requires the additional deployment of a large number of sensor nodes for context recognition. The scheme recognizes the mentioned attack situations; however, it is not possible to accurately identify compromised nodes. In addition, a high-spec node used as a CH node is required. In this case, the network user cannot randomly arrange the nodes because the CH and member nodes must be properly arranged to form a cluster.

B. Temporal Logic based abnormal behavior detection of node

We introduce an algorithm for detecting abnormal behavior based on TL and statistics to detect false reports and compromised nodes and clusters in massive attacks. This section describes the overall scenario for detection using the proposed scheme.

The verification node stores TL rules for the normal transition of events detected. If the contents of the report sent by the verification node to the BS performs a state transition that is contrary to the TL rule, the node that transmits the report determines that the node has been attacked. Each node monitors state transitions in real-time. This proposed scheme was implemented based on a fire event detection scenario. Nodes placed in the field have three states based on temperature: Normal, On Fire, and Done. Such a state is a value that can be determined through the temperature and humidity sensor and various other sensor modules. Sensing technologies are beyond the scope of this paper. The rules for fire variation used in the scenario are as follows.

TABLE I. TL RULES FOR FIRE DISASTER DETECTION

no	*Definition*	*Explanation*
1	□ (On Fire → ○ Done)	If a node senses Fire, the next moment in time will be Done.
2	Normal → ◇ Done	If the time of a node of Normal state flows infinitely, then the state will eventually be Done.
3	□ (Done → ○ Done)	If the present is Done, then all future moments is Done.
4	□ (Normal → ○ (Normal ∨ On Fire))	If the present is Normal, the next moment is Normal or On Fire.

The fire spread used in the experiment is defined in three states as shown in Table 1. The simple false report randomly generated by an attacker will be detected and filtered according to the TL rule. For example, a node with a Normal state cannot transition to the Done state without transitioning through the On Fire state.

The TL-based node detects abnormal behavior. However, we assumed that the attacker could perform an intelligent attack without causing an unlogical state transition. As a countermeasure for this situation, we introduced a statistics-based ranking algorithm to prevent advanced attacks. The statistics-based ranking algorithm ranks the state transition of nodes by unit time. If the BS detects the lowest priority state transition of a node, the BS is selected as a suspicious node. The report is filtered when suspicious nodes are observed to be repeatedly performing low-ranking state transitions. The following table shows the process of detecting compromised nodes through the proposed scheme.

Algorithm 1: Compromised node detection

```
M ← MAX_UT
N ←Number of nodes, MAX_UT initialize by network field
for n←0 to N do
  set node[n].T to 0
end for
for i ←0 to M do
  for n←0 to N do
    if node[n].state is abnormal state for i
      set node[n].tag to true
    else
     if node[n].probability is abnormal state
       set node[n].T to T+1
     else continue
end for
    if node[n].tagcount > MAX_UT
     set node[n].compromised to true
end for
```

The TL rule was used as the rule for state transition, and the probability of state transition was applied for each unit time to improve the attack detection rate and reduce the false detection rate for normal nodes in the proposed scheme.

TL rules represent the normal situation process that occurs in the domain. However, if the attacker has expertise of the domain, they can exploit it to attempt various types of attacks. In addition, if a rule of a simple pattern of state transition is stored, abnormal behaviors that do not violate them can be detected. Such attacks cannot be detected with the existing TL rules. Therefore, the proposed scheme additionally uses a ranking algorithm to prevent such an intelligent attack. The ranking algorithm is described in detail in Section 3.3.

C. CA-based statistical ranking algorithm

This chapter describes the overall detection scenario by applying the statistical ranking algorithm and the proposed scheme to detect intelligent attacks that cannot be detected by the TL rule.

In this scenario, the TL rule contains the normal state transition for the fire progression in a CA-based simulation. If the state transition of a suspicious attack node actually shows behavior contrary to the TL rule, the node is judged as a compromised node. The proposed scheme is applied to the simulation by fusion with the existing CA-based fire prediction model. When the BS determines that the node is a suspicious attack node, the BS compares the state value between a neighbor node of the suspicious attack and the node with the lowest probability of mutation at each unit time. If the values are the same, the BS increases the Attack Doubt Tag count. When it reaches the preset threshold, it is regarded as an attacking node. Therefore, when an attack situation is detected using the fire prediction model, a network administrator can prevent node attacks by adjusting the detection threshold of the proposed scheme.

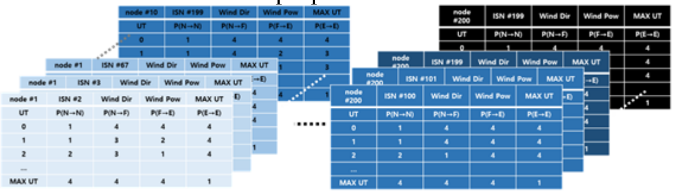
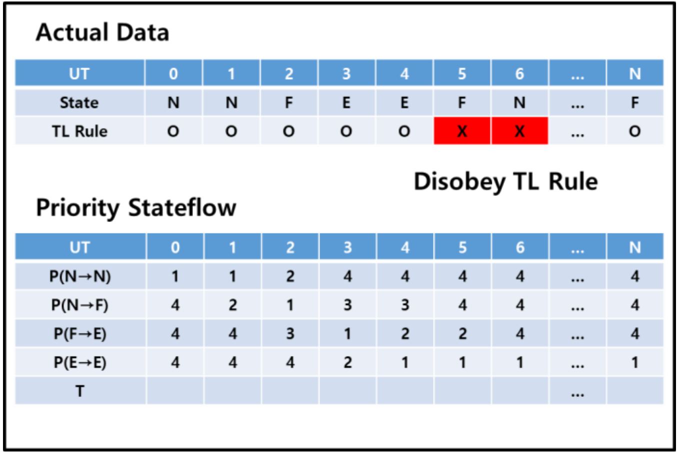


Fig. 4. Node state value and transition probability measurement data stored in the BS

The ranking statistics of the state transition by fire spreading according to time were obtained through virtual simulation as shown in Fig. 4.

The BS measures the state value of the fire progress and the state transition probability according to the wind direction, wind speed, and location of the initial fire generating node through simulation, and stores the information. The transition probability is stored according to the unit time elapsed from the initial fire point; the larger the field size, the larger the unit time progress.

The BS stores the state transition value for each unit time of each node and the ranking value for the state transition. Therefore, the compromised node is inferred by comparing the report data that comes in real-time through the information. In this scenario, the sensor node uses four state transitions.



Actual Data

UT	0	1	2	3	4	5	6	...	N
State	N	N	F	E	E	F	N	...	F
TL Rule	O	O	O	O	O	X	X	...	O

Disobey TL Rule

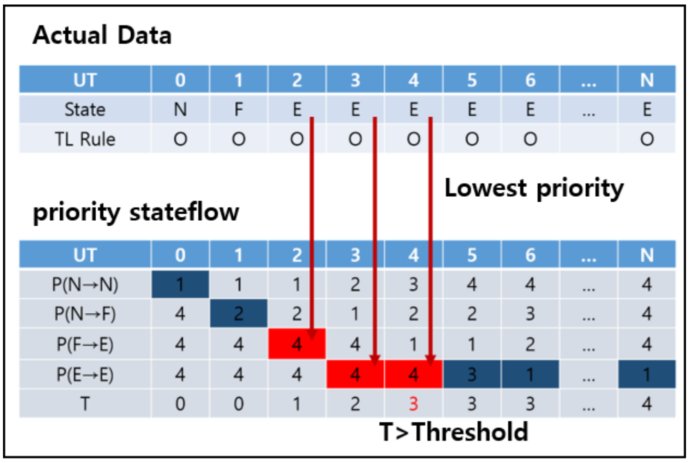
Priority Stateflow

UT	0	1	2	3	4	5	6	...	N
P(N→N)	1	1	2	4	4	4	4	...	4
P(N→F)	4	2	1	3	3	4	4	...	4
P(F→E)	4	4	3	1	2	2	4	...	4
P(E→E)	4	4	4	2	1	1	1	...	1
T								...	

Fig. 5. Malicious attack node detection using TL

Only normal state transitions were considered in our experiment. Therefore, it is possible to detect a suspicious attack node through a security model that includes this state transition knowledge.

Fig. 5 illustrates the compromising detection process of a node that violates the predefined TL rule. In the proposed scheme, an action that violates the TL rule is regarded as an attacking node immediately without setting an individual rank threshold. If normal data that does not violate the TL rule is introduced, a data comparison is performed for reliability verification as shown in Fig. 6 and 7.



Actual Data

UT	0	1	2	3	4	5	6	...	N
State	N	F	E	E	E	E	E	...	E
TL Rule	O	O	O	O	O	O	O		O

Lowest priority

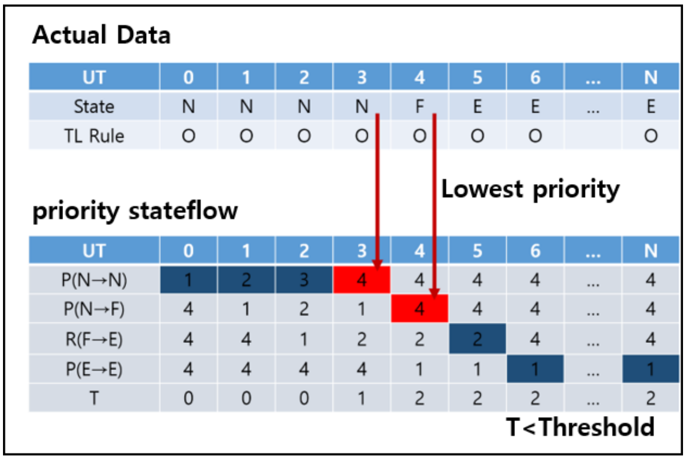
priority stateflow

UT	0	1	2	3	4	5	6	...	N
P(N→N)	1	1	1	2	3	4	4	...	4
P(N→F)	4	2	2	1	2	2	3	...	4
P(F→E)	4	4	4	4	1	1	2	...	4
P(E→E)	4	4	4	4	4	3	1	...	1
T	0	0	1	2	3	3	3	...	4

T>Threshold

Fig. 6. Data comparison for intelligent attack detection in a rank table (actual data > preset threshold)

Fig. 6 represents a ranking-based abnormal node detection table. When the UT is 2, 3, and 4, the node has the lowest probability of state transition. If the value received by the BS is 4, the T value becomes greater than the preset threshold. In this case, the BS determines that the source node that created the report has been corrupted.



Actual Data

UT	0	1	2	3	4	5	6	...	N
State	N	N	N	N	F	E	E	...	E
TL Rule	O	O	O	O	O	O	O		O

Lowest priority

priority stateflow

UT	0	1	2	3	4	5	6	...	N
P(N→N)	1	2	3	4	4	4	4	...	4
P(N→F)	4	1	2	1	4	4	4	...	4
R(F→E)	4	4	1	2	2	2	4	...	4
P(E→E)	4	4	4	4	1	1	1	...	1
T	0	0	0	1	2	2	2	...	2

T<Threshold

Fig. 7. Data comparison for intelligent attack detection in a rank table (actual data < preset threshold)

Fig. 7 shows the two lowest priorities in the state flow table; however, the node is considered to be normal because it performed abnormal behavior less than the threshold.

Statistics-based detection requires a threshold value because there may be a mistake in judgment as an attack on a normal state transition. If the threshold is set too low, the abnormal behavior observed by the normal node is regarded as an attack too quickly, and the event detection rate may be reduced because the node cannot be used anymore.

IV. EXPERIMENT

A. Experiment Parameters

TABLE II. EXPERIMENT PARAMETERS

Item	***Value***
Sensor field size (m*m)	1000 × 1000
Number of sensor nodes	1000 – 36000
Transmission range (m) Cluster size	80 40 – 60

B. Assumptions

An experiment of the proposed scheme was performed assuming that the MAC value included in all false reports arriving at the BS is valid. Attack attempts that repeatedly transmit a random state and an intelligent attack that shows a state transition that does not violate the TL rule were used. Since the TL-based node abnormal behavior detection scheme was performed at the BS, there was no extra cost by the additional inference algorithm. To compare the filtering performance with the MAC-based security protocol, we compare the performance of PVFS and the proposed scheme. In this experiment, the number of nodes deployed in the field may vary according to the size of the field, and the UT value, which is the unit time from the start to the end of the fire, varies from 10 to 15. The graph considers all cases of the minimum field size to the maximum field size.

C. Experimental result

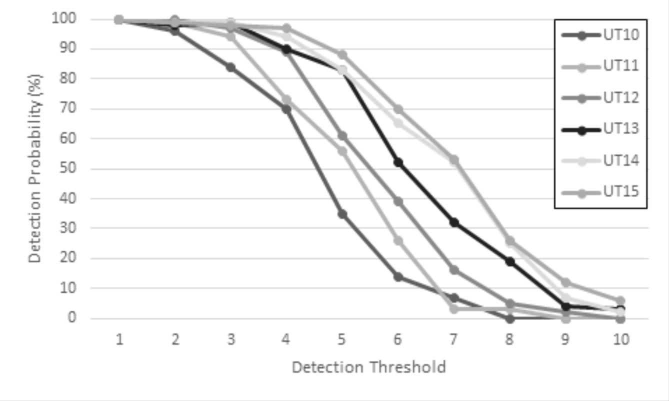


Fig. 8. Simple attack detection rate according to UT and the detection threshold

An attacker can execute a simple attack that repeatedly sends a random state that does not follow the TL rules. Fig. 8 shows the detection rate applying a TL-based security that blocks simple attacks according to the threshold values. Unintelligent random attacks show a fairly high detection rate even with TL-based detection. In addition, the detection rate rapidly decreases from the moment when a certain threshold value is exceeded, regardless of the size of the field. Through this experiment, the simple pattern attacks can achieve sufficient results even with TL rule-based security with an appropriate detection threshold. However, if an attack with a pattern that does not violate the TL rule occurs because of an intelligent attack, the detection rate of the TL-based rule decreases rapidly. Therefore, a TL-based, statistics-based security should be considered.

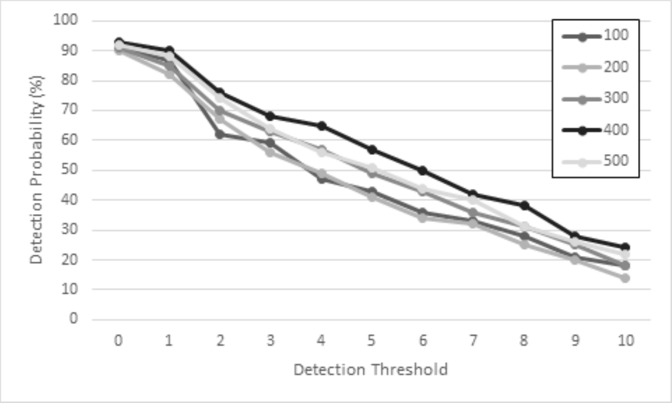


Fig. 9. Detection accuracy according to the number of nodes and threshold

Fig. 9 shows the detection rate according to the detection threshold that detects intelligent attacks with a TL-based statistics-based security algorithm. In addition, the number of nodes may be different depending on the size of the complete field, and the experiment was conducted with various comparisons of the number of CH nodes from 100 to 500. Experimental results show that when the threshold is between 0 and 1, the most efficient detection is possible with an average detection rate of 90.056%. As shown in Fig. 9 and 10, there was no significant difference in the detection accuracy from the number of nodes deployed in the field, and this shows that the proposed detection scheme can efficiently detect regardless of the size of the field.

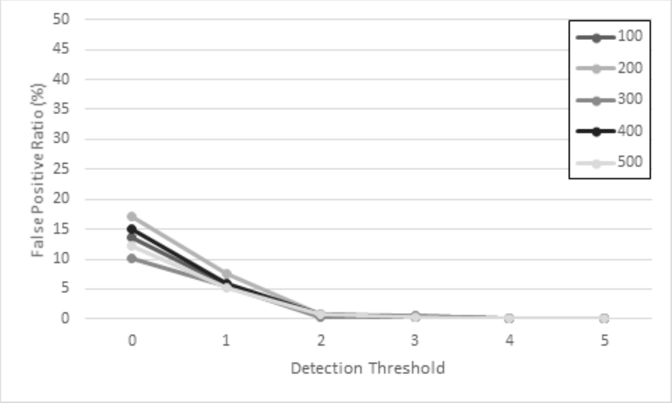


Fig. 10. Normal event false positive rate according to the number of nodes and threshold

Fig. 10 illustrates the probability that the proposed detection method falsely detects a normal event as an attack according to the number of CH nodes deployed in the virtual field and threshold value. Since normal events can display behaviors that deviate from statistics, there is a high probability of false positives as attacks when the detection threshold is extremely low. When the threshold value is 0, an average of 10.794% of event false detection is observed, and when the threshold value is 1, the false detection rate is 4.749%. When the threshold value is greater than 2, the false detection rate drops significantly to less than 1%. In addition, it is possible to check the false positive rate that is largely independent of the size of the field and the number of nodes. As shown in Fig. 9 and 10, the proposed scheme can be expected to show a maximum efficiency between the thresholds of 0 – 3. In addition, the false positive rate and attack detection rate are in a trade-off relationship, and it will be important to set the threshold value suitable for the network administrator.

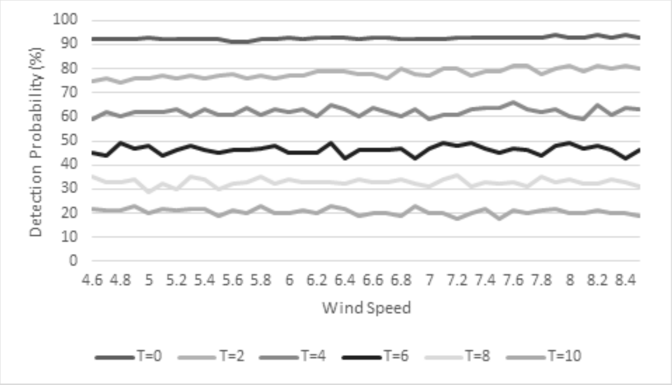


Fig. 11. Attack detection rate according to wind speed

Fig. 11 represents the detection rate by threshold according to the wind speed in the field. The proposed scheme shows a constant performance that is not affected by the wind speed. In addition, when the ranking threshold is different, the detection algorithm of the proposed scheme does not require additional information and a MAC, other than the information contained in the existing report, so there is no additional cost.

V. CONCLUSION

This paper introduces how to achieve situational awareness and security based on the contents of the report. We applied a ranking algorithm based on statistics through simulation and TL rules for massive attack situations that cannot be achieved in the existing application layer protocol. En-route security protocols are not secure when large nodes are compromised; however, the vulnerability can be supplemented through this proposed scheme. We describe the performance analysis of the proposed scheme by assuming a fire scenario. In addition, the intelligent attack solution using the ranking algorithm based on collecting statistical data through a highly reliable CA-based simulation was also considered. Moreover, the model is able to apply appropriate TL rules and statistics to the WSN field for monitoring other situations, such as tank movement and rider movement, in addition to fire conditions. In future work, we will conduct research on an algorithm to determine a threshold value that is more accurate and suitable for constructing the WSN environment of network users through interworking with a neural network-based predictive model for fire transition.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (No. NRF-2018R1D1A1B07048961).

REFERENCES

[1] Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks."Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM, 2006.

[2] Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004

[3] Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004

[4] Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005

[5] X. Yang et al., ″A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems,″ IEEE Trans. Comput., vol. 64, no. 1, pp. 4–18, Jan. 2015.

[6] Yang, Hao, et al. "Toward resilient security in wireless sensor networks." Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. 2005.

[7] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys and Tutorials, 15(4), 2046–2069.

[8] Yu, Bo, and Bin Xiao. "Detecting selective forwarding attacks in wireless sensor networks." Proceedings 20th IEEE international parallel & distributed processing symposium. IEEE, 2006.

[9] Bauer, Kevin, et al. "Low-resource routing attacks against tor." Proceedings of the 2007 ACM workshop on Privacy in electronic society. 2007.

[10] Pnueli, Amir. "The temporal logic of programs." 18th Annual Symposium on Foundations of Computer Science (sfcs 1977). IEEE, 1977.

[11] Manna, Zohar, and Amir Pnueli. The temporal logic of reactive and concurrent systems: Specification. Springer Science & Business Media, 2012.

[12] Fisher, Michael. An introduction to practical formal methods using temporal logic. Vol. 82. Hoboken: Wiley, 2011.

[13] Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.

[14] Jung Sub Ahn, & Tae Ho Cho. "Fuzzy Logic Optimization Method for Energy Efficiency Improvement of CFFS using GA in WSN" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, No. 6, pp. 474 - 480, Aug. 2020.

[15] Nam, Su Man, and Tae Ho Cho. "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks." IEEE Transactions on Mobile Computing 16.10 (2017): 2751-2763