# INTERNATIONAL SCIENCE REVIEWS

AIU

No. 2 (1) 2020

Natural Sciences and Technologies series

www.aiu.kz

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

# INTERNATIONAL SCIENCE REVIEWS
# Natural Sciences and Technologies series

*Has been published since 2020*

## №2 (1) 2020

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz



**International Sciense Reviews NST - 76153**
**International Science Reviews**
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

# CONTENT

# ELLO FLOOD ATTACK AND WAYS OF PROTECTION IN WIRELESS SENSOR NETWORKS

**Zhukabayeva T.K., Abdildayeva A.A., Mardenov E.M.**

**Annotation.** There are many vulnerabilities to attack in wireless sensor networks. Wireless sensor network has become an important application of the paradigm of special networks, for example, for monitoring the physical environment. These sensor networks have limitations on system resources such as battery power, communication range, and processing capabilities. Low computing power and wireless connectivity make these networks vulnerable to various types of network attacks. One of them is the hello flood attack, in which an attacker who is not a legal host on the network can send a hello request to any legitimate host and violate the security of WSN. The current solutions for these types of attacks are mainly cryptographic, which suffer from high computational complexity. Therefore, they are less suitable for wireless sensor networks.

**Keywords:** Wireless Sensor Network; hello flood attack; attack detection;

## INTRODUCTION

The importance of using FSU is growing every year. This is directly related to the increasing need for monitoring, monitoring, measurement and solving many other operational problems in such areas as industry, medicine, commerce, science, and everyday life. The most famous applications of FSU: military equipment, medicine, environmental programs, household appliances, etc. [1].

The Wireless Sensor Network (WSN) consists of thousands of dedicated sensor nodes with processing, transmission and storage capabilities, as well as computing capabilities. Security is becoming a serious concern for many mission-critical applications that wireless sensor networks are supposed to support. By their nature, the vulnerable characteristics of WSNs make them susceptible to various types of attacks.


Picture 1. Classification of attacks on the WSN.

There are various types of attacks that threaten LEACH services: Sybil attack, black hole, selective forwarding and Hello hello attack. Hello flood attack is one of the

main attacks at the WSN network layer. The welcome attack is caused by an attacker with a high transmission power who can send or play welcome packets, which are used to detect neighbors. Thus, an attacker creates the illusion of proximity to other nodes, and the main routing protocol may be violated, which facilitates further types of attacks. An attacker transmits packets with such high power that a large number of nodes in the network select it as the parent node. Figure 2 shows a Hello flood attack scenario.

Figure-2 Hello flood –attack

All messages that will be broadcast to the WSN are routed through this parent, which increases the delay. An attacker sends these welcome messages to a large number of nodes in a wide WSN area. Then these nodes must be convinced that the attacker's node in the network is their neighbor. All nodes will respond to this HELLO message from an attacker and will spend their energy. This leads to confusion in the WSN. Figures 3 a and b show a Hello flood attack on the network. In this diagram, circles, a rectangle, and a triangle represent the nodes of the sensor, base station, and attacker, respectively.

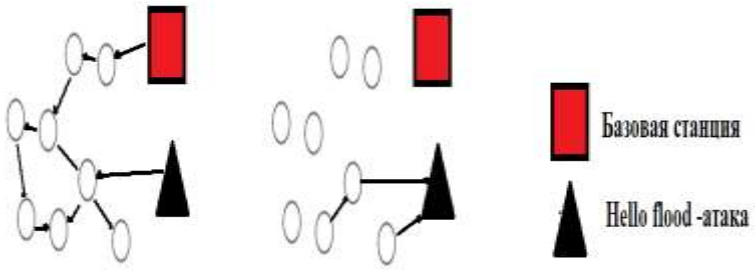


Figure 3 - Hello flood attack

a) Shows the transmission of hello packets by an attacker with a higher transmission power than the base station.

b) shows legitimate nodes that consider the attacker to be their neighbor

In the message “Hello, flood” captures the sensor node, broadcasts greeting messages on the network and proclaims itself to be their neighbor. When any node on

the network receives this greeting message, it assumes that the sender node is in the communication range, and starts transmitting this node and makes an entry in its routing table as a neighbor. All sensor nodes communicate with the base station through their neighbors. When an attacker captures a legitimate node in the network or creates a fake node, he sends a greeting message to all nodes in the network with high power, this creates confusion that the message comes from neighboring nodes. Thus, all nodes in the network assume that the hello message path is the shortest path from the base station, assuming that the attacker (malicious) node is the base station and begins communication with the attacker. Thus, an attacker can control the network, since the base station is completely disconnected from the WSN, and also affects its routing. Hello flood attack is one of the main attacks at the network level in WSN.

Hello flood attack support

A large number of attacks are supported by a hello attack, including flooding, hardening and grabbing a node, false replication of a node, etc. These auxiliary attacks are described below:

*1) Flood*

In a flood attack, the attacker continually sends a new connection request to his neighbor in order to seize resources. This leads to severe resource constraints for legitimate sites.

*2) Quenching and capture of the node*

Falsification is associated with attacks on components, which include changing the internal structure of a single chip. Consultations can easily capture him and can be used to attack hi flood. Host capture attacks give an attacker full control over the sensor host, but host capture is not so simple. To capture a site, an attacker requires expert knowledge, as well as expensive equipment and other resources. Complex is the removal of nodes from the network for a large amount of time.

*3) False node replication*

In an attack with a false replication of a node, an attacker implants a new touch node using a legitimate user identifier. The attacker first removes the legitimate node from the network and at this point deploys the false. This false node replication can lead to huge destruction in the WSN, supporting a complimentary flow attack. An attacker can control the entire network most of the time, so the damage from this attack is very large

## SUGGESTED METHODS AGAINST HELLO FLOOD ATTACK

In [2], a technology was proposed for sending data over multipath base stations, in which the sensor node supports the number of different secrets (keys) in a multiple tree. Using these secrets, the sensor node can forward its detected data to multiple routes. There are several base stations in the network that control a certain number of nodes, and there are also general communication tools between the base stations. Each base station has all the secrets that are shared by all the sensor nodes covered by it, in accordance with the key assignment protocol. Given the shared secret and the

generated new key between the two nodes of the sensor, the route configuration process requires a lot of processing, therefore, it is inefficient.

In [3], the authors proposed a security solution structure adapted to the base station for protection against DoS attacks. After the initial discovery of DoS, the base station offers customers cryptographic puzzles to protect themselves from various types of attacks. Compared to traditional puzzle schemes, they introduce new reputation-based client puzzles that apply a dynamic policy to adjust the complexity of the puzzle for each node in terms of the value of the node's reputation. Consequently, the punishment for malicious nodes becomes more and more urgent without imposing unnecessary unnecessary burdens on most ordinary nodes.

In [4], the author suggests that greetings can be counteracted by an "identity verification protocol". This protocol checks the bidirectionality of a channel with an encrypted echo-return mechanism before taking meaningful actions based on the message received from this link. This defense mechanism becomes effective when the attacker has a highly sensitive receiver and a powerful transmitter. If an attacker compromises a node before the feedback message, it can block all of its descending nodes by simply discarding the feedback messages. Thus, such an attacker can easily create a wormhole for each node within reach. Since the connections between these nodes and the attacker are bidirectional, the approach described above is unlikely to locally detect or prevent a "greeting".

Given the lack of energy resources of the sensor nodes, the authors proposed in [5] a probabilistic approach, which forces several randomly selected nodes to inform the base station about greeting requests. The base station then further analyzes the authentication request.

In [5], the cryptographic method is used to prevent a greeting attack. Any two sensors have the same secret key. Each new encryption key is generated on the fly during communication. This phenomenon ensures that only reachable nodes can decrypt and verify the message and, therefore, prevent an attacker from attacking the network. But the main drawback of this approach is that any attacker can fake his identity and then generate attacks.

[6] This article proposes a non-cryptographic solution for HELLO flood detection, which does not. once the test packet is transmitted is greatly reduced. The simulation results showed the detection of adversary nodes with minimal communication costs, since the number of test packets sent for detection decreases from 20-35 to 10-14 (approx.). A non-cryptographic solution for detecting a HELLO attack is proposed in this article, which does not. once the test packet is transmitted is greatly reduced. The simulation results showed the detection of adversary nodes with minimal communication costs, since the number of test packets sent for detection decreases from 20-35 to 10-14 (approx.). A non-cryptographic solution for detecting a HELLO attack is proposed in this article, which does not. once the test packet is transmitted is greatly reduced. The simulation results showed the detection of adversary nodes with minimal communication costs, since the number of test packets sent for detection decreases from 20-35 to 10-14 (approx.).

A security mechanism based on signal strength and geographical information was proposed in [7] to detect malicious nodes that trigger hi-flood and wormhole attacks. The idea is to compare the level of the receive signal with its expected value calculated using geographic information and a predetermined transceiver specification. The frequency of detection of a solution depends on various parameters, such as network density, the transmit power multiplier of the malicious node, the probability of checking the message, etc.

## SUGGESTED ALGORITHM

This project aims to provide a simple and convenient way to generate simulations and deploy malicious nodes for the wireless sensor network (WSN), which uses the routing protocol for low-power and lossy devices (RPL) as the network layer.

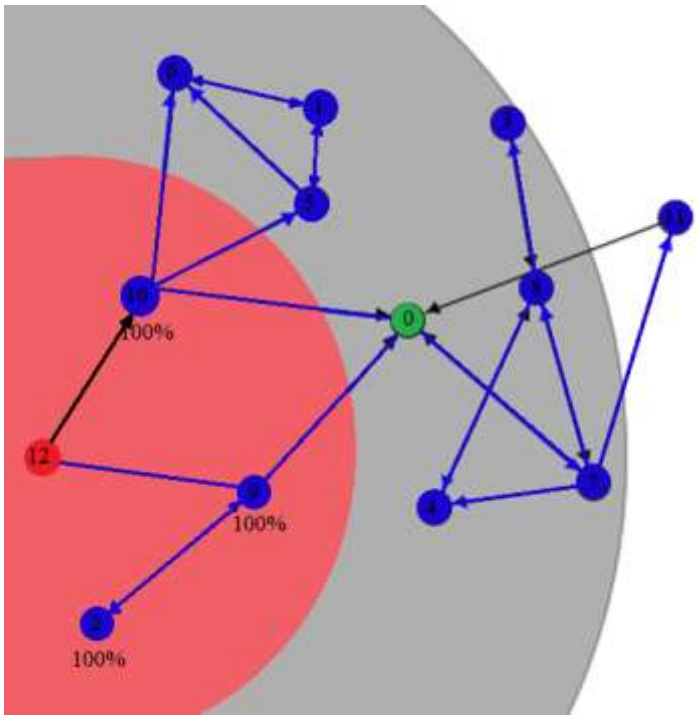


Figure 5. General Hello Flood Attack Model

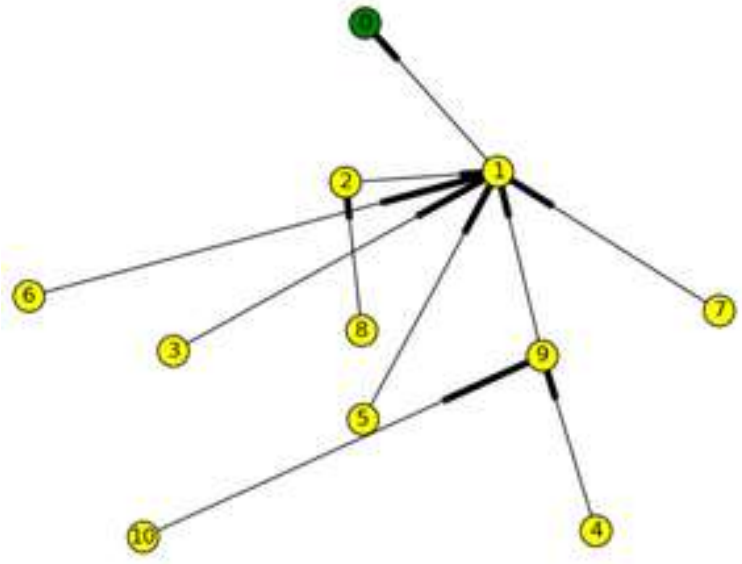


Figure 6. Hello Flood attacks in a node

```
{
  "BASE": {
    "simulation": {
      "number_motes": 10,
      "target": "z1",
      "duration": 300
    },
  },
  "test1": {
    "simulation": {
      "title": "Test simulation",
      "goal": "Create a new simulation",
      "notes": ""
    },
    "malicious": {
      "type": "sensor",
      "building-blocks": [
        "sinkhole"
      ]
    }
  },
  "test2": {
    "simulation": {
      "title": "Another test simulation",
      "goal": "Create another new simulation",
      "notes": "",
    },
    "malicious": {
      "type": "sensor",
      "building-blocks": [
        "hello-flood"
      ]
    }
  }
}
```

Figure 7. Program code

## CONCLUSIONS

Security plays a crucial role in the proper functioning of wireless sensor networks. Our proposed security structure for detecting greetings using the signal and the client puzzle method requires less processing power and energy and, therefore, is quite suitable for sensor networks.

Based on existing work, most researchers are trying to find ICT solutions for the detection, identification and resistance to failures in the FSU. The researchers used a different intrusion detection scheme. Very few researchers have been able to test their security system using a true FSU. Also, some results showed a low detection rate. The future solution must be verified in a real sensor network. Thanks to such a check, it will be easy to check whether their solutions correspond to the available BSS resources.

## REFERENCES

1. Ефименко, М. С. Беспроводные сенсорные сети / М. С. Ефименко, С. И. Клымив, Р. Б. Саткенов. — Текст : непосредственный, электронный // Молодой ученый. — 2018. — № 51 (237). — С. 40-42. — URL: https://moluch.ru/archive/237/55115/ (дата обращения: 13.04.2020).
2. A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT
3. Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu, Liyong Tang , (2006), Enhancing Base Station Security against DoS Attacks in Wireless Sensor Networks, IEEE
4. Venkata C. Giruka, Mukesh Singhal, James Royalty, Srilekha Varanasi, (2006), Security in wireless networks, Wiley Inter Science
5. Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE
6. S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, pp. 193-198.
7. Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, (2004), Malicious Node Detection in Wireless Sensor Networks, IEEE
8. Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, May 2012, A Cross-Layer Based Intrusion Detection Technique for Wireless Networks, The International Arab Journal of Information Technology, Vol. 9, No. 3.
9. Nusrat Fatema, Remus Brad, December 2013, Attacks and counterattacks on wireless sensor networks, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6.
10. Kaur, Reenkamal & Sachdeva, Monika. (2018). Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks. 10.1007/978-981-10-6005-2_40

## ELLO FLOOD ATTACK И СПОСОБЫ ЗАЩИТЫ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

**Жукабаева Т.К., Абдилдаева А.А., Марденов Е.М.**

**Аннотация**. Существует множество уязвимостей для атак в беспроводных сенсорных сетях. Беспроводная сенсорная сеть стала важным приложением парадигмы специальных сетей, например, для мониторинга физической среды. Эти сенсорные сети имеют ограничения на системные ресурсы, такие как заряд

батареи, дальность связи и возможности обработки. Низкая вычислительная мощность и беспроводная связь делают эти сети уязвимыми для различных типов сетевых атак. Одним из них является атака приветствия, при которой злоумышленник, не являющийся законным хостом в сети, может отправить запрос приветствия любому легитимному хосту и нарушить безопасность WSN. Текущие решения для этих типов атак в основном криптографические, которые страдают от высокой вычислительной сложности. Поэтому они менее подходят для беспроводных сенсорных сетей.

**Ключевые слова:** беспроводная сенсорная сеть; привет атака наводнения; обнаружение атаки;

**Information about the authors:** Zhukabayeva T.K[1]., Abdildayeva A.A[2]., Mardenov E.M[1].
[1]Astana International University, Eurasian National University named after L.N. Gumilyov, Nur Sultan, Republic of Kazakhstan, **tamara_kokenovna@mail.ru**
[2]Astana International University, Nur Sultan, Republic of Kazakhstan, abass_81@mail.ru
[3]Astana International University, Eurasian National University named after L.N. Gumilyov, Nur Sultan, Republic of Kazakhstan emardenov@gmail.com