An enhanced AES-GCM based security protocol for securing the IoT communication

A.B. Feroz Khan1,2, S. Kalpana Devi2, K. Rama Devi3

1 Syed Hameedha Arts and Science College, Kilakarai, Ramanathapuram, 623806, India
2 RV University, Bengaluru, 560059, India
3 Panimalar Engineering College, Chennai, 600069, India

abferozkhan@gmail.com2, https://orcid.org/0000-0002-9395-9493
kalpanasubramaniam2010@gmail.com, https://orcid.org/0000-0001-7049-3144
ramadevi.sarav@gmail.com, https://orcid.org/0000-0002-6431-8363

Abstract

In the recent years, the devices in Internet of Things (IoT) are growing exponentially due to the emergence of many sophisticated applications. This tremendous growth leads to serious security challenges and the devices of Wireless Sensor Networks should be protected from various attacks. IoT can be configured dynamically without fixed infrastructure and the devices are communicated with one another in an Ad-hoc manner. The work presents the classification of various DDoS attacks in the IoT environment and provides a solution for replay attack. All variations of DDoS attacks are modeled using UML based activity modeling. This clearly understands the behavior of each version of attacks and their performance in the environment. The modeling also helps to construct a solution to prevent this attack from its execution. The work also proposed a trust based protocol for replay attacks which allows the attack inside the network and blocks it after identifying the attack based on its specific behavior. The network performance is improved after implementing this proposed protocol inside the network with help of simulation under realistic conditions. The performance metrics considered in the work are energy, packet loss, computational time and throughput. The paper compares the performance with the state-of-the-art schemes such as Efficient Distributed Deterministic Key and Hash-based Message Authentication Code. The experimental analysis proved that the proposed scheme outperforms the other state-of-the-works in terms of computational cost, throughput, and delay.

Keywords

DDoS, security, trusted metrics, IoT


УДК 004.75

Усовершенствованный протокол безопасности на основе AES-GCM для защиты связи в интернете вещей

А.Б. Фероз Хан1,2, Деви С. Калпана2, К. Рама Деви3

1 Колледж искусств и науки Сайеда Хамидхи, Раманатхапурам, 623806, Индия
2 Университет RV, Бангалор, 560059, Индия
3 Панималарский инженерный колледж, Ченнаи, 600069, Индия

abferozkhan@gmail.com2, https://orcid.org/0000-0002-9395-9493
kalpanasubramaniam2010@gmail.com, https://orcid.org/0000-0001-7049-3144
ramadevi.sarav@gmail.com, https://orcid.org/0000-0002-6431-8363

Аннотация

В последние годы количество устройств в интернете вещей (IoT) растет в геометрической прогрессии из-за появления множества сложных приложений. Это приводит к серьезным проблемам безопасности. Устройства
Wireless Sensor Network (WSN) должны быть защищены от различных атак. Интернет вещей можно настраивать динамически без фиксированной инфраструктуры, а устройства WSN взаимодействуют друг с другом в режиме прямо беспроводного динамического соединения (Ad-hoc). Представлена классификация различных Distributed Denial of Service (DDoS)-атак в среде интернета вещей и предложено решение для предотвращения повторной атаки. Выполнено моделирование DDoS-атак с использованием UML-диаграмм активности, что дает четкое понимание поведения каждой версии атаки и их производительности в среде. В результате моделирования построено решение, предотвращающее выполнение атак. Предложен протокол, основанный на доверии, для анализа поведения повторных атак, который допускает атаку внутри сети и блокирует ее после идентификации. Проведено моделирование в реальных условиях для улучшения производительности сети. Рассмотрены показатели производительности сети: энергия, потеря пакетов, время вычислений и пропускная способность. Проведено сравнение производительности сети предложенного решения с современными схемами, такими как EDDK и HMAC. Экспериментальный анализ показал, что предложенный протокол превосходит схемы EDDK и HMAC по параметрам вычислительных затрат, пропускной способности и задержки.

**Key words**
DDoS, безопасность, надежные показатели, интернет вещей

**Citation**
With the continued increase of IoT devices, strong security policies must be implemented to ensure confidentiality, integrity, and availability — the three core principles of security. Collaboration between governments and industry players is crucial to establish these policies which should prioritize end-to-end security to combat automated and distributed attacks such as DDoS. The security of IoT components as a whole must be taken into account, rather than individual components. Advanced standards that support global interoperability and enhance IoT security must also be developed. The policies must be established with government and industrial collaboration based on the following considerations [6].

— To combat automated and distributed attacks like DDoS, end-to-end security measures must be implemented in IoT systems.
— The security of IoT systems must be viewed holistically, rather than solely focusing on individual components, to ensure that potential vulnerabilities in the overall network are identified and addressed.
— Advanced standards that establish a core baseline are required to support worldwide interoperability and strengthen IoT security.

The rest of the paper is divided into four parts: the literature review of various related works for the detection of node capturing attack, the introduction of the proposed work and its novelty compared to other works, the discussion of the results of the proposed work, and the conclusion.

Related works

After analyzing various countermeasures available against DDoS attacks, it is observed that reactive, proactive, and mobile agent countermeasures are the most common techniques used for protection. Reactive technique starts its protection mechanism only after encountering an attack, whereas proactive techniques set up a secure channel before the attack is executed to prevent it from happening. Mobile agent techniques are used in sensor nodes to act as a defensive mechanism and save the network from DDoS attacks. Several research works have proposed different methods to detect and prevent jamming attacks in wireless networks.

Verma et al. [7] proposed a detection technique using timing information and signal strength to detect jamming attacks. However, their proposed scheme works well in combination with other countermeasures. Fadele et al. [8] proposed a Countermeasure Detection and Consistency Algorithm technique that uses signal strength and location information to detect reactive jamming attacks. However, their work increases the computational cost and consumes more energy. Jia et al. [9] proposed a stakelberg game approach to address the anti-jamming problem. Their proposed method is well-suited to overcome jamming issues but it increases energy and implementation costs.

In addition to the aforementioned works, Korzhuk V. et al. [10] proposed the “Identification of Attacks against Wireless Sensor Networks Based on Behaviour Analysis”. This paper presents a method for detecting attacks against WSNs by analyzing their behavior. Their approach focuses on identifying patterns and anomalies in network behavior to identify potential attacks. By leveraging behavior analysis techniques, their method offers a promising approach to detecting attacks in WSN.

Yao [11] proposed a multi-agent method that uses a Bernaola Galvan Segmentation Algorithm (BGSA) algorithm to reduce the effect of external jamming attacks. Gezici et al. [12] proposed an optimum jammer placement problem to detect the presence of jammer nodes, using timing, and location information. Sun et al. [13] proposed a multi-data flow topology scheme for mobile jamming attacks, which effectively prevents jamming in the network using routing information in the secret path. Muralleedharan and Osadciw [14] proposed a defensive method that mitigates jamming attacks using receiver operating characteristics. However, their method increases energy and computational costs. Strasser et al. [15] proposed a reactive technique for detecting jamming attacks using different approaches, but their proposed method works best with more than one detection technique. Sasikala and Rengarajan [16] proposed using an artificial bee colony to detect jamming attacks on wireless networks. Their work uses different performance metrics, such as packet loss rate, energy, and Received Signal Strength, to provide an efficient anti-jamming technique. Existing works in the field of DDoS attack detection and mitigation for securing communication in IoT networks have made significant contributions to enhancing the security of IoT devices. These works have focused on developing techniques and protocols to identify and prevent various types of attacks, such as jamming attacks, replay attacks, and other forms of DDoS attacks. Table 1 summarizes the details of the main parameters used in the existing works with their advantages and disadvantages.

From Table 1, we observed that the contributions of existing works have significantly advanced the field of DDoS attack detection and mitigation in IoT networks. These works have improved the security, reliability, and performance of IoT devices, paving the way for secure deployment and utilization of IoT technologies in various domains. Therefore, all the related works discussed in the literature section perform well in detecting and preventing jamming attacks. However, most of these proposed schemes work well in combination with other detection schemes, and this may result in more overhead on resource-constrained devices in IoT. In the evaluation of our proposed work, it is observed that our scheme efficiently detects and prevents jamming attacks, improving the network performance in terms of energy, delay, computational cost, and the variable number of malicious nodes.

The proposed protocol

The proposed solution presents a trust-based security protocol that can detect and isolate DDoS attacks effectively while aiming to achieve strong security at a reduced time and cost. The computational process used in the solution is based on a few parameters to improve efficiency. Since the network layer is a critical component of the network responsible for addressing and packet delivery, attackers often target this layer to redirect packets to their desired...
An enhanced AES-GCM based security protocol for securing the IoT communication

<table>
<thead>
<tr>
<th>Related Work</th>
<th>Main Parameters</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verma et al. [7]</td>
<td>Timing information, signal strength</td>
<td>Effective detection of jamming attacks</td>
<td>Works best in combination with other countermeasures</td>
</tr>
<tr>
<td>Fadele et al. [8]</td>
<td>Signal strength, location information</td>
<td>Reactive jamming attack detection</td>
<td>Increased computational cost and energy consumption</td>
</tr>
<tr>
<td>Jia et al. [9]</td>
<td>Stakelberg game approach</td>
<td>Anti-jamming solution</td>
<td>Increased energy and implementation costs</td>
</tr>
<tr>
<td>Korzhuk et al. [10]</td>
<td>Behavior analysis</td>
<td>Effective technique for identifying attacks based on machine learning algorithms, Study of the dependence of accuracy on confidence level and a priori probability of the normal state</td>
<td>Reliance on a complex machine learning algorithm (Random Forest) may require significant computational resources and training data, potentially limiting its practical deployment in resource-constrained IoT devices or networks.</td>
</tr>
<tr>
<td>Yao [11]</td>
<td>BGSA algorithm</td>
<td>Reduction of external jamming attacks</td>
<td>Not suitable for all types of jamming scenarios</td>
</tr>
<tr>
<td>Gezici et al. [12]</td>
<td>Timing, location information</td>
<td>Optimum jammer placement detection</td>
<td>Limited to specific scenarios and network conditions</td>
</tr>
<tr>
<td>Sun et al. [13]</td>
<td>Multi-data flow topology</td>
<td>Effective prevention of mobile jamming attacks</td>
<td>Increased complexity and configuration overhead</td>
</tr>
<tr>
<td>Muraleedharan and Osadciw [14]</td>
<td>Receiver operating characteristics</td>
<td>Mitigation of jamming attacks</td>
<td>Higher energy and computational costs</td>
</tr>
<tr>
<td>Strasser et al. [15]</td>
<td>Reactive jamming detection</td>
<td>Wide range of detection approaches</td>
<td>Works best with multiple detection techniques</td>
</tr>
<tr>
<td>Sasikala and Rengarajan [16]</td>
<td>Artificial bee colony algorithm</td>
<td>Efficient anti-jamming technique</td>
<td>Performance impact on resource-constrained devices</td>
</tr>
</tbody>
</table>

### Table 1. Summary of related works

**Overview of the proposed protocol**

The proposed protocol aims to authenticate devices before allowing them to exchange data with other devices in the network. The network consists of two phases: the first phase involves generating a trusted value that serves as a ticket for device communication. The trust value is calculated based on the number of successful and failed interactions of a node $i$ with other nodes. A successful interaction increases the trustworthiness score, while a failed interaction decreases it. Direct trust $DT_{ij}$ is the trustworthiness score of node $j$ as perceived by node $i$ based on their direct interactions. Indirect trust $IT_{ij}$ is the trustworthiness score of node $j$ as perceived by node $i$ based on the recommendations of other nodes in the network. A successful interaction increases the trustworthiness score, while a failed interaction decreases it. The trustworthiness score can be calculated as follows:

$$T_i = \frac{S_i + F_i}{S_i - F_i}$$

where $S_i$ is the number of successful interactions of node $i$, and $F_i$ is the number of failed interactions.

Direct trust $DT_{ij}$: It is the trustworthiness score of node $j$ as perceived by node $i$ based on their direct interactions. The direct trust can be calculated using the following equation:

$$DT_{ij} = T_j.$$

Indirect trust $IT_{ij}$: It is the trustworthiness score of node $j$ as perceived by node $i$ based on the recommendations of other nodes in the network. The indirect trust can be calculated using the following equation:
\[ IT_{ij} = (1 - w)T_j + w(\text{SUM}_k(T_kR_{kj})/\text{SUM}_k(R_{kj})), \]

where \( w \) is a weighting factor that determines the importance of the recommendations, \( R_{kj} \) is the recommendation of node \( k \) for node \( j \), and the \( \text{SUM} \) is taken over all nodes \( k \) that have recommended node \( j \).

The above equation helps to find a malicious node by calculating its Trusted Value (TV). The TV is based on several metrics, such as packet forwarding ratio, residual energy, and hop count. If a node TV falls below a certain threshold, it is considered untrusted, and its packets are not forwarded in the network. When a node TV falls below the threshold, it is moved to the “suspicious” state. In this state, the node is monitored to see if it continues to behave maliciously. If the node behavior improves and its TV rises above the threshold, it is moved back to the “normal” state. However, if the node behavior remains suspicious or worsens, it is moved to the “attack” state and is removed from the network.

The presented work proposes a trust-based protocol for device authentication in IoT networks. The protocol generates a trust value based on device ID, access rights, and a random key, which is used as a ticket for device communication. The protocol contains two phases: trust value calculation and AES_GCM-based encryption. The encryption method involved in the protocol ensures authentication and confidentiality of the ticket, and both devices are mutually authenticated before communication.

The paper analyzes the various types of attacks possible in each layer of IoT communication and identifies DDoS attacks as the most catastrophic. UML activity modeling is used to understand the behavior of each attack and propose a solution. Replay attack is identified as the most damaging DDoS attack as it minimizes throughput and maximizes delay, leading to increased energy consumption. The attack is executed using a vulnerable node which becomes a jammer node if successful. The jammer node senses the channel for availability and sends data continuously to jam the network, making detection challenging and leading to performance degradation. While many security solutions have been proposed, they are not efficient for the IoT environment, reducing network performance in terms of energy, delay, and computational cost. The proposed protocol addresses these issues by reducing computational cost, energy consumption, and delay. To combat the various types of DDoS attacks, different countermeasures have been proposed in the literature. Some of the commonly used countermeasures include filtering, rate-limiting, and packet-marking techniques. However, these techniques have certain limitations, such as high overhead, complexity, and reduced network performance. In recent years, trust-based security protocols have gained popularity as a promising approach for protecting IoT devices from DDoS attacks. These protocols ensure mutual authentication of devices before allowing data transmission between them. By establishing a trust value for each device based on factors, such as device ID, random key, and access rights, the protocol ensures that only trusted devices can access the network. The proposed trust-based protocol discussed earlier uses AES_GCM-based encryption technique to protect the trust value from attackers. This protocol provides both authentication and confidentiality, making it an efficient solution for securing IoT networks. In addition to trust-based security protocols, UML modeling has also
been used to analyze the different variations of DDoS attacks and develop new solutions to prevent them. By identifying the behavior of different attacks, researchers have been able to propose more effective countermeasures to protect IoT networks. One of the most catastrophic attacks in IoT communication is the DDoS attack [17] which can bring the entire network down. Replay attack, which minimizes throughput and maximizes time delay by rapidly increasing energy consumption, is considered the most important attack among all the variations of DDoS attacks [18, 19]. This attack can severely damage the performance of the network and should be prevented at all costs. To detect replay attacks, various techniques, such as watchdog timers, sequence numbers, and hash chains have been proposed. However, these techniques have limitations, such as high overhead and complexity. In recent years, machine learning techniques, such as clustering and decision trees, have also been explored for detecting and preventing DDoS attacks in IoT networks [20]. Overall, protecting IoT networks from DDoS attacks requires a multi-faceted approach that involves using efficient security protocols, analyzing attack behavior, and implementing effective countermeasures. By adopting these approaches, we can ensure the security and reliability of IoT networks while minimizing the cost and energy consumption.

**Results discussion**

The proposed work was implemented and evaluated through simulations in a real-time scenario. The performance of the system was analyzed in terms of energy consumption, delay, and throughput across different time intervals. The simulations were conducted in two sets; the first set evaluated the system performance under varying traffic intervals, while the second set considered the presence of malicious nodes in the network. To analyze the system performance under different traffic conditions, intervals ranging from 1 s to 10 s were used, where 1 s was considered as fast and 10 s as slow. The simulation parameters used in the evaluation are presented in Table 2.

Fig. 3, a, b, c depict the results obtained from the proposed TBC approach, which measures energy, delay, and throughput based on traffic intervals ranging from 1 s to 10 s. The outcomes clearly demonstrate that Threshold Based Countermeasure (TBC) outperforms energy Efficient Distributed Deterministic Key (EDDK) and Hash-based Message Authentication Code (HMAC) in terms of energy consumption during DDoS attacks. This is due to the fact that TBC identifies and eliminates malicious nodes, thereby saving energy that could otherwise be wasted by those nodes. Additionally, TBC yields the lowest delay, as it effectively detects and isolates attacks, enabling other nodes to continue their operations without any unnecessary delays. A single node execution of an attack can result in its spread to multiple nodes in the network causing other nodes to wait longer to access the channel. After implementing TBC, the waiting time for nodes in the network is reduced, resulting in an increase in throughput under non-attack conditions.

Fig. 3, d, e depict the results of simulations conducted to evaluate the performance of the proposed solution under realistic conditions with respect to energy and delay considerations. The simulation was conducted by

<table>
<thead>
<tr>
<th>Table 2. Simulation parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Network Area</td>
</tr>
<tr>
<td>Number of nodes</td>
</tr>
<tr>
<td>Radio Range, m</td>
</tr>
<tr>
<td>Transmission Range, m</td>
</tr>
<tr>
<td>Bandwidth, Mbps</td>
</tr>
<tr>
<td>MAC Protocol</td>
</tr>
<tr>
<td>Routing Protocol</td>
</tr>
<tr>
<td>Traffic Type</td>
</tr>
<tr>
<td>Packet Size, B</td>
</tr>
<tr>
<td>Simulation Time, s</td>
</tr>
<tr>
<td>Mobility Model</td>
</tr>
<tr>
<td>Pause Time, s</td>
</tr>
<tr>
<td>Traffic Intervals</td>
</tr>
<tr>
<td>Attacker Nodes</td>
</tr>
<tr>
<td>Performance Metrics</td>
</tr>
</tbody>
</table>

![Fig. 3. Performance analysis of the proposed work. Energy Comparative Analyzes: power consumption (a), average delay (b) and throughput (c) of EDDK, HMAC and TBC. Average power consumption by malicious nodes (d), analysis of average latency by malicious nodes (e)](image)
A.B. Feroz Khan, S. Kalpana Devi, K. Rama Devi

The proposed work introduces a trusted-based protocol to tackle DDoS attacks in the network. The protocol mandates that each node should possess a trusted value before accessing any device in the network. Only trusted nodes are allowed to participate in the communication process. Nodes can be in one of three states: normal, suspicious, or attack. Suspicious and attack states are used to identify potential attacks. If any node is confirmed as an attacker based on trusted metrics, it is immediately removed from the network. The multi-hop path analysis process, which is initiated once a suspicious node is confirmed, is a key feature of the proposed work. The evaluation results demonstrate that the proposed work...

**Fig. 3.** Performance analysis of the proposed work. Energy Comparative Analysis: power consumption (a), average delay (b) and throughput (c) of EDDK, HMAC and TBC. Average power consumption by malicious nodes (d), analysis of average latency by malicious nodes (e)
outperforms existing methods in terms of energy, delay, and throughput. The proposed protocol has shown a reduction in energy consumption by approximately 15% compared to existing solutions. The work also revealed a decrease in average delay by approximately 20% and the increased throughput of 10% when employing the proposed protocol. By promptly identifying and isolating DDoS attacks, unnecessary delays in packet delivery are minimized enabling smoother communication among nodes in the network. As future work, we aim to investigate our approach effectiveness against different types of jamming attacks. This would help to expand the scope of the research and demonstrate the protocol potential in a wider range of scenarios.

References

Литература

Authors

A.B. Feroz Khan — PhD, Assistant Professor, Syed Hameedha Arts and Science College, Kilakarai, Ramanathapuram, 623806, India, sc 57209466258, https://orcid.org/0000-0002-9395-9493, abferozkhan@gmail.com
S. Kalpana Devi — Assistant Professor, RV University, Bangaluru, 560059, India, sc 57211952643, https://orcid.org/0000-0001-7049-3144, Kalpanasubramaniyan2010@gmail.com
K. Rama Devi — PhD, Associate Professor, Panimalar Engineering College, Chennai, 600069, India, sc 56708714800, https://orcid.org/0000-0002-6431-8363, ramadevi.sarav@gmail.com

Received 15.11.2022
Approved after reviewing 21.05.2023
Accepted 26.07.2023

Авторы

Фероз Хан А.Б. — PhD, доцент, Колледж искусств и науки Сейда Хамидхи, Раманатхапурам, 623806, Индия, sc 57209466258, https://orcid.org/0000-0002-9395-9493, abferozkhan@gmail.com
Калпана Деви С. — доцент, Университет RV, Бангалор, 560059, Индия, sc 57211952643, https://orcid.org/0000-0001-7049-3144, Kalpanasubramaniyan2010@gmail.com
Рама Деви К. — PhD, доцент, Панималарский инженерный колледж, Ченнаи, 600069, Индия, sc 56708714800, https://orcid.org/0000-0002-6431-8363, ramadevi.sarav@gmail.com

Статья поступила в редакцию 15.11.2022
Одобрена после рецензирования 21.05.2023
Принята к печати 26.07.2023

Работа доступна по лицензии Creative Commons «Attribution-NonCommercial»