НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2023 Том 23 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2023 Vol. 23 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2023-23-4-711-719

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

A.B. Feroz Khan[1]✉, S. Kalpana Devi[2], K. Rama Devi[3]

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

[1] abferozkhan@gmail.com✉, https://orcid.org/0000-0002-9395-9493
[2] kalpanasubramaniyan2010@gmail.com, https://orcid.org/0000-0001-7049-3144
[3] 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

For citation: Feroz Khan A.B., Kalpana Devi S., Rama Devi K. An enhanced AES-GCM based security protocol for securing the IoT communication. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 4, pp. 711–719. doi: 10.17586/2226-1494-2023-23-4-711-719

УДК 004.75

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

А.Б. Фероз Хан[1]✉, Деви С. Калпана[2], К. Рама Деви[3]

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

[1] abferozkhan@gmail.com✉, https://orcid.org/0000-0002-9395-9493
[2] kalpanasubramaniyan2010@gmail.com, https://orcid.org/0000-0001-7049-3144
[3] 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 прямого 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 производительность 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.

Ключевые слова
DDoS, безопасность, надежные показатели, интернет вещей

Ссылка для цитирования: Фероз Хан А.Б., Калпана Деви С., Рама Деви К. Усовершенствованный протокол безопасности на основе AES-GCM для защиты связи в интернете вещей // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 4. С. 711–719 (на англ. яз.). doi: 10.17586/2226-1494-2023-23-4-711-719

Introduction

The Internet of Things (IoT) is a vast network of interconnected smart devices that can be found all over the world. These devices are equipped with sensors that allow them to measure their surroundings and communicate with other devices over the internet [1, 2]. The IoT is a network of connected smart devices that can transfer data to one another. These devices include sensors, actuators, Radio Frequency IDentification and Wireless Sensor Network (WSN) components, and other technologies that make life easier in various fields, such as healthcare, agriculture, education, transportation, and more. However, the increase in IoT applications has also led to security challenges that need to be addressed.

Protecting the privacy of users is crucial since sensitive and important data is often transmitted through these smart applications. While there are currently available security solutions, they fall short in fully meeting all the security requirements of smart applications. These solutions tend to focus only on functionality requirements, and do not integrate well with the entire system. Therefore, there is a need for integrated security solutions that comply with different standards and technologies to ensure the security of smart applications [3, 4]. Fig. 1 depicts the architecture of IoT. The protection of communication channels is a primary security requirement in safeguarding of IoT devices, given that physical attacks pose critical threats to sensor nodes deployed in various environments. To address the significant harm that Distributed Denial of Service (DDoS) attacks can cause in IoT networks, this study presents a proposed solution. Multiple works have emerged to prevent DDoS attacks in IoT, which typically involve an attacker turning a normal node into a “zombie” and spreading the attack to other nodes in the network. The zombie node then interacts with other nodes in the cluster as if they were normal, even allowing it to share confidential information without the network knowledge [5].

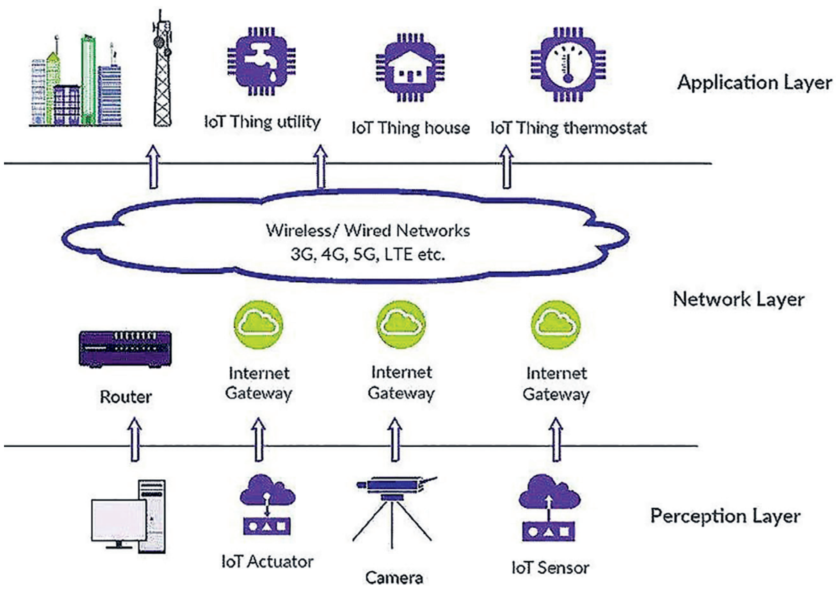


Fig. 1. Overview of IoT communication

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. Muraleedharan 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 the 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

Table 1. Summary of related works

Related Work	Main Parameters	Advantages	Disadvantages
Verma et al. [7]	Timing information, signal strength	Effective detection of jamming attacks	Works best in combination with other countermeasures
Fadele et al. [8]	Signal strength, location information	Reactive jamming attack detection	Increased computational cost and energy consumption
Jia et al. [9]	Stakelberg game approach	Anti-jamming solution	Increased energy and implementation costs
Korzhuk et al. [10]	Behavior analysis	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	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.
Yao [11]	BGSA algorithm	Reduction of external jamming attacks	Not suitable for all types of jamming scenarios
Gezici et al. [12]	Timing, location information	Optimum jammer placement detection	Limited to specific scenarios and network conditions
Sun et al. [13]	Multi-data flow topology	Effective prevention of mobile jamming attacks	Increased complexity and configuration overhead
Muraleedharan and Osadciw [14]	Receiver operating characteristics	Mitigation of jamming attacks	Higher energy and computational costs
Strasser et al. [15]	Reactive jamming detection	Wide range of detection approaches	Works best with multiple detection techniques
Sasikala and Rengarajan [16]	Artificial bee colony algorithm	Efficient anti-jamming technique	Performance impact on resource-constrained devices

destination. The proposed solution addresses this issue with a trust-based detection protocol designed to protect IoT devices from various types of DDoS attacks.

Overview of the proposed protocol

The proposed protocol aims to authenticate devices before allowing them to exchange data with other devices in the network as in Fig. 2.

In Fig. 2, the variables ID_1, ID_2 are identifier of the device, $Rights_1$, $Rights_2$ are the access rights of the devices, E_K refers to encryption key, r refers to random number and H refers to Hash function. The proposed solution introduces a trust-based security protocol designed to effectively detect and isolate DDoS attacks while striving for strong security with reduced time and cost. For better understanding of the Fig. 2, the work is divided into following logical parts:

— The proposed protocol aims to authenticate devices before allowing them to exchange data with other devices in the network. It achieves this by generating a trusted value that serves as a ticket for device communication. The trust value is calculated based on the device ID, a random key, and the access rights. The protocol consists of two phases. In the first phase, the trust value is calculated using the device ID, random number, and access rights. The second phase involves applying an AES_GCM-based encryption technique to encrypt the trusted metrics. The random number generated in the process helps protect the network from forgery.

— Once the trust value is established, it is hashed and encrypted with a public key. The proposed protocol also introduces the concept of trustworthiness score T_i, which 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:

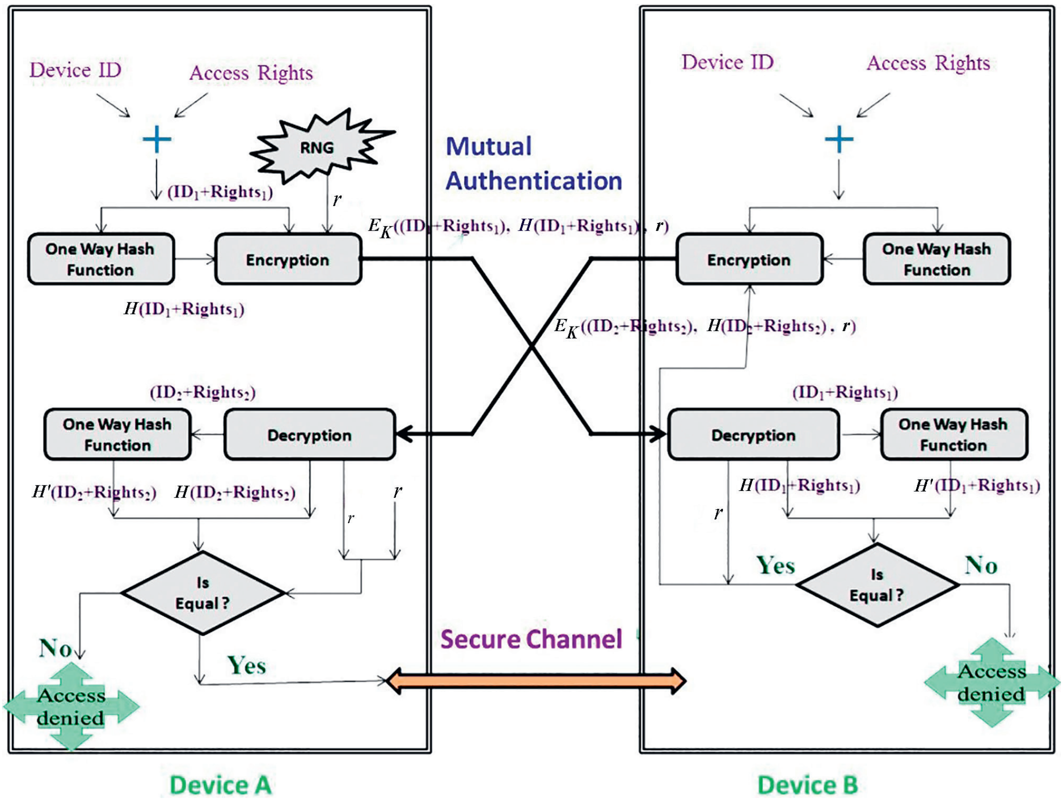


Fig. 2. The Proposed Protocol Architecture

$$IT_{ij} = (1 - w)T_j + w(SUM_k(T_kR_{kj})/SUM_k(Rk_j)),$$

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 *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

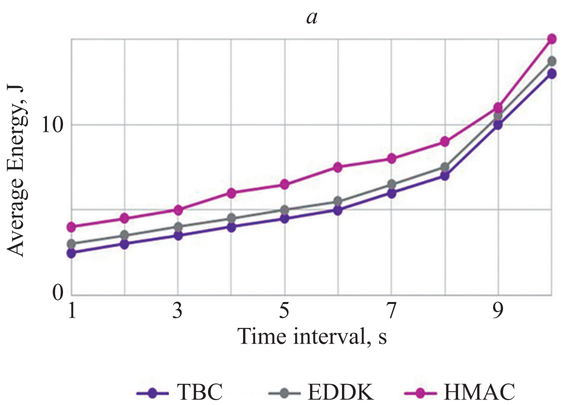
The proposed work was implemented and evaluated through simulations in a real-time scenario. The performance of the system was analyzed in terms of energy consumption, delay, and throughput across different time intervals. The simulations were conducted in two sets; the first set evaluated the system 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.

Table 2. Simulation parameters

Parameter	Value
Network Area	1000 m × 1000 m
Number of nodes	100
Radio Range, m	250
Transmission Range, m	100
Bandwidth, Mbps	2
MAC Protocol	IEEE 802.11
Routing Protocol	AODV
Traffic Type	CBR (Constant Bit Rate)
Packet Size, B	512
Simulation Time, s	100
Mobility Model	Random Waypoint
Pause Time, s	30
Traffic Intervals	1 s to 10 s
Attacker Nodes	2 to 20
Performance Metrics	Energy, Delay, and Throughput

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



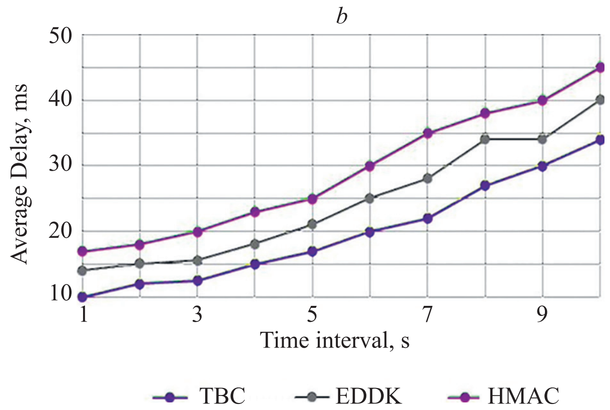


Fig. 3. Performance analysis of the proposed work. Energy Comparative Analyzes: power consumption (*a*), average delay (*b*) and throughput (*c*) of EDDK, HMAC and TBC. Average power consumption by malicious nodes (*d*), analysis of average latency by malicious nodes (*e*)

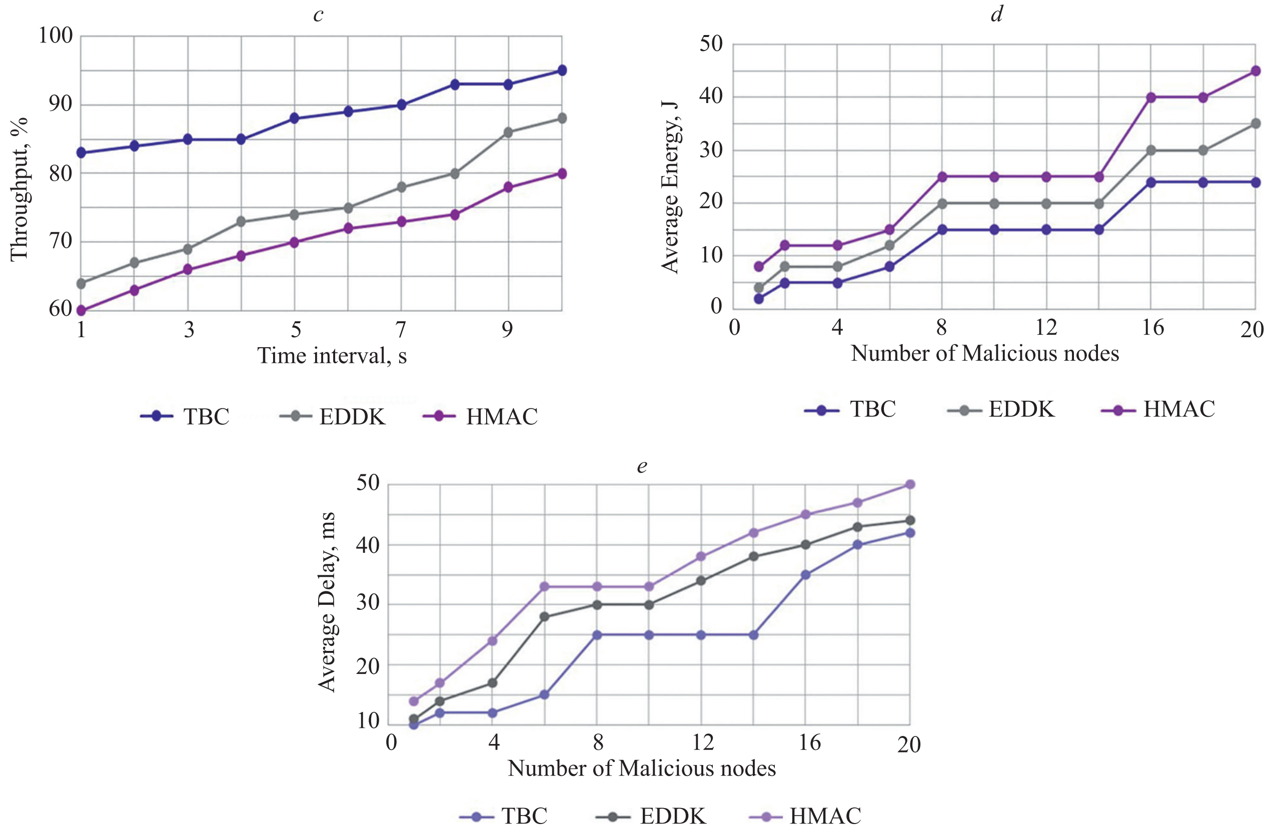


Fig. 3. Performance analysis of the proposed work. Energy Comparative Analyzes: power consumption (*a*), average delay (*b*) and throughput (*c*) of EDDK, HMAC and TBC. Average power consumption by malicious nodes (*d*), analysis of average latency by malicious nodes (*e*)

introducing varying numbers of malicious nodes in the network while keeping the total number of nodes constant at 100. The number of attacker nodes ranged from 2 to 20. The improved performance of the proposed solution can be attributed to its ability to effectively detect and remove attacks from the network through its unique features including cross-layer capabilities, reduced false detections, and node cooperation. It was observed that introducing a trade-off between the severity of the attack and its detectability reduces the performance of the optimal strategy, and the performance of the considered optimal model deteriorates as the number of attacks in the network increases. Moreover, the proposed algorithm increases energy consumption only under node mobility conditions. The performance of the work is evaluated in NS-2 which is a widely used discrete event network simulator that allows researchers to simulate and evaluate various network protocols and algorithms. In the context of the proposed work, NS-2 was used to simulate a WSN and evaluate the performance of the proposed TBC algorithm in terms of energy, delay, and throughput under various traffic intervals and different numbers of malicious nodes. The network topology, traffic patterns, and simulation parameters are defined using the NS-2 script. They then ran the simulation to collect performance metrics, such as energy consumption, delay, and throughput, which were used to evaluate the effectiveness of the proposed TBC algorithm. The simulation was conducted in two sets. In the first set, the researchers evaluated the performance of the proposed TBC algorithm under various traffic intervals ranging from 1 s to 10 s. The simulation parameters were specified in a table, and the results were plotted in Fig. 3, *a*, *b*, *c*. In the second set, the researchers evaluated the performance of the proposed TBC algorithm by varying the number of malicious nodes in the network. The simulation was conducted with 100 nodes, and the number of attacker nodes added in the network ranged from 2 to 20. The simulation results were plotted in Fig. 3, *d*, *e*. Overall, NS-2 was used to simulate and evaluate the performance of the proposed TBC algorithm in a controlled environment, which allowed the researchers to analyze the effectiveness of the algorithm under different scenarios and conditions.

Conclusion

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 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

1. Rao N.S.V., Poole S.W., Ma C.Y.T., He F., Zhuang J., Yau D.K.Y. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models. *Risk Analysis*, 2016, vol. 35, no. 4, pp. 602–616. https://doi.org/10.1111/risa.12362
2. Wang J., Yang G., Sun Y., Chen S. Defending against Sybil attacks based on received signal strength in wireless sensor networks. *Chinese Journal of Electronics*, 2008, vol. 17, no. 4, pp. 611–614.
3. Khan G.A., Anandharaj G. A Cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. *Wireless Personal Communications*, 2021, vol. 119, no. 4, pp. 3149–3159. https://doi.org/10.1007/s11277-021-08391-6
4. Meena U., Sharma A. Secure key agreement with rekeying using FLSO routing protocol in wireless sensor network. *Wireless Personal Communications*, 2018, vol. 101, no. 2, pp. 1177–1199. https://doi.org/10.1007/s11277-018-5755-9
5. Renold A.P., Ganesh A.B. Energy efficient secure data collection with path-constrained mobile sink in duty-cycled unattended wireless sensor network. *Pervasive and Mobile Computing*, 2019, vol. 55, pp. 1–12. https://doi.org/10.1016/j.pmcj.2019.02.002
6. Vasudeva A., Sood M. Survey on sybil attack defense mechanisms in wireless ad hoc networks. *Journal of Network and Computer Applications*, 2018, vol. 120, pp. 78–118. https://doi.org/10.1016/j.jnca.2018.07.006
7. Verma R., Darak S.J., Tikkiwal V., Joshi H., Kumar R. Countermeasures against jamming attack in sensor networks with timing and power constraints. *Proc. of the 11th International Conference on Communication Systems & Networks (COMSNETS)*, 2019, pp. 485–488. https://doi.org/10.1109/comsnets.2019.8711437
8. Fadele A.A., Othman M., Hashem I.A.T., Yaqoob I., Imran M., Shoaib M. A novel countermeasure technique for reactive jamming attack in internet of things. *Multimedia Tools and Applications*, 2019, vol. 78, no. 21, pp. 29899–29920. https://doi.org/10.1007/s11042-018-6684-z
9. Jia L., Xu Y., Sun Y., Feng S., Anpalagan A. Stackelberg game approaches for anti-jamming defence in wireless networks. *IEEE Wireless Communications*, 2018, vol. 25, no. 6, pp. 120–128. https://doi.org/10.1109/mwc.2017.1700363
10. Korzhuk V., Groznykh A., Menshikov A., Strecker M. Identification of attacks against wireless sensor networks based on behaviour analysis. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 2019, vol. 10, no. 2, pp. 1–21. https://doi.org/10.22667/JOWUA.2019.06.30.001
11. Yao Y., Xiao B., Wu G., Liu X., Yu Z., Zhang K., Zhou X. Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI. *IEEE Transactions on Mobile Computing*, 2019, vol. 18, no. 2, pp. 362–375. https://doi.org/10.1109/tmc.2018.2833849
12. Gezici S., Bayram S., Kurt M.N., Gholami M.R. Optimal jammer placement in wireless localization systems. *IEEE Transactions on Signal Processing*, 2016, vol. 64, no. 17, pp. 4534–4549. https://doi.org/10.1109/tsp.2016.2552503
13. Sun H., Chen C., Hsu S. Mobile jamming attack and its countermeasure in wireless sensor networks. *Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, 2017, pp. 457–462. https://doi.org/10.1109/ainaw.2007.255
14. Muraleedharan R., Osadciw L.A. Jamming attack detection and countermeasures in wireless sensor network using ant system. *Proceedings of SPIE*, 2006, vol. 6248, pp. 62480G. https://doi.org/10.1117/12.666330
15. Strasser M., Danev B., Čapkun S. Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks*, 2010, vol. 7, no. 2, pp. 1–29. https://doi.org/10.1145/1824766.1824772

Литература

1. Rao N.S.V., Poole S.W., Ma C.Y.T., He F., Zhuang J., Yau D.K.Y. Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models // Risk Analysis. 2016. V. 35. N 4. P. 602–616. https://doi.org/10.1111/risa.12362
2. Wang J., Yang G., Sun Y., Chen S. Defending against Sybil attacks based on received signal strength in wireless sensor networks // Chinese Journal of Electronics. 2008. V. 17. N 4. P. 611–614.
3. Khan G.A., Anandharaj G. A Cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT // Wireless Personal Communications. 2021. V. 119. N 4. P. 3149–3159. https://doi.org/10.1007/s11277-021-08391-6
4. Meena U., Sharma A. Secure key agreement with rekeying using FLSO routing protocol in wireless sensor network // Wireless Personal Communications. 2018. V. 101. N 2. P. 1177–1199. https://doi.org/10.1007/s11277-018-5755-9
5. Renold A.P., Ganesh A.B. Energy efficient secure data collection with path-constrained mobile sink in duty-cycled unattended wireless sensor network // Pervasive and Mobile Computing. 2019. V. 55. P. 1–12. https://doi.org/10.1016/j.pmcj.2019.02.002
6. Vasudeva A., Sood M. Survey on sybil attack defense mechanisms in wireless ad hoc networks // Journal of Network and Computer Applications. 2018. V. 120. P. 78–118. https://doi.org/10.1016/j.jnca.2018.07.006
7. Verma R., Darak S.J., Tikkiwal V., Joshi H., Kumar R. Countermeasures against jamming attack in sensor networks with timing and power constraints // Proc. of the 11th International Conference on Communication Systems & Networks (COMSNETS). 2019. P. 485–488. https://doi.org/10.1109/comsnets.2019.8711437
8. Fadele A.A., Othman M., Hashem I.A.T., Yaqoob I., Imran M., Shoaib M. A novel countermeasure technique for reactive jamming attack in internet of things // Multimedia Tools and Applications. 2019. V. 78. N 21. P. 29899–29920. https://doi.org/10.1007/s11042-018-6684-z
9. Jia L., Xu Y., Sun Y., Feng S., Anpalagan A. Stackelberg game approaches for anti-jamming defence in wireless networks // IEEE Wireless Communications. 2018. V. 25. N 6. P. 120–128. https://doi.org/10.1109/mwc.2017.1700363
10. Korzhuk V., Groznykh A., Menshikov A., Strecker M. Identification of attacks against wireless sensor networks based on behaviour analysis // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). 2019. V. 10. N 2. P. 1–21. https://doi.org/10.22667/JOWUA.2019.06.30.001
11. Yao Y., Xiao B., Wu G., Liu X., Yu Z., Zhang K., Zhou X. Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI // IEEE Transactions on Mobile Computing. 2019. V. 18. N 2. P. 362–375. https://doi.org/10.1109/tmc.2018.2833849
12. Gezici S., Bayram S., Kurt M.N., Gholami M.R. Optimal jammer placement in wireless localization systems // IEEE Transactions on Signal Processing. 2016. V. 64. N 17. P. 4534–4549. https://doi.org/10.1109/tsp.2016.2552503
13. Sun H., Chen C., Hsu S. Mobile jamming attack and its countermeasure in wireless sensor networks // Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07). 2017. P. 457–462. https://doi.org/10.1109/ainaw.2007.255
14. Muraleedharan R., Osadciw L.A. Jamming attack detection and countermeasures in wireless sensor network using ant system // Proceedings of SPIE. 2006. V. 6248. P. 62480G. https://doi.org/10.1117/12.666330
15. Strasser M., Danev B., Čapkun S. Detection of reactive jamming in sensor networks // ACM Transactions on Sensor Networks. 2010. V. 7. N 2. P. 1–29. https://doi.org/10.1145/1824766.1824772

16. Sasikala E., Rengarajan N. An intelligent technique to detect jamming attack in wireless sensor networks (WSNs). *International Journal of Fuzzy Systems*, 2015, vol. 17, no. 1, pp. 76–83. https://doi.org/10.1007/s40815-015-0009-4
17. Alaba F.A., Awodele O., Afolabi I. Security challenges in internet of things (IoT) enabled healthcare systems. *Proc. of the 2017 International Conference on Computing Networking and Informatics.* IEEE, 2017, pp. 1–7.
18. Kumar P.H., AnandhaMala G.S. HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment. *Journal of Supercomputing*, 2023, vol. 79, no. 3, pp. 3181–3209. https://doi.org/10.1007/s11227-022-04714-x
19. Zhang X., He J., Wei Q. EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2011, no. 1, pp. 765143. https://doi.org/10.1155/2011/765143
20. Chaganti R., Bhushan B., Ravi V. A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. *Computer Communications*, 2023, vol. 197, pp. 96–112. https://doi.org/10.1016/j.comcom.2022.10.026

16. Sasikala E., Rengarajan N. An intelligent technique to detect jamming attack in wireless sensor networks (WSNs) // International Journal of Fuzzy Systems. 2015. V. 17. N 1. P. 76–83. https://doi.org/10.1007/s40815-015-0009-4
17. Alaba F.A., Awodele O., Afolabi I. Security challenges in internet of things (IoT) enabled healthcare systems // Proc. of the 2017 International Conference on Computing Networking and Informatics. IEEE, 2017. P. 1–7.
18. Kumar P.H., AnandhaMala G.S. HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment // Journal of Supercomputing. 2023. V. 79. N 3. P. 3181–3209. https://doi.org/10.1007/s11227-022-04714-x
19. Zhang X., He J., Wei Q. EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks // EURASIP Journal on Wireless Communications and Networking. 2011. N 1. P. 765143. https://doi.org/10.1155/2011/765143
20. Chaganti R., Bhushan B., Ravi V. A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions // Computer Communications. 2023. V. 197. P. 96–112. https://doi.org/10.1016/j.comcom.2022.10.026

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

Авторы

Фероз Хан А.Б. — PhD, доцент, Колледж искусств и науки Сайеда 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

Received 15.11.2022
Approved after reviewing 21.05.2023
Accepted 26.07.2023

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