НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2022 Том 22 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2022 Vol. 22 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2022-22-6-1127-1135

A multi-path secure routing for the detection of node capturing attack in wireless sensor network

Jayaraman Kolangiappan[1]✉, Angamuthu Senthil Kumar[2]

[1] Department of Computer Science, Periyar University, Salem, 636011, India
[2] Department of Computer Science, Arignar Anna Government Arts College, Namakkal, 637002, India

[1] jkakshiya@gmail.com✉, https://orcid.org/0000-0001-5093-5822
[2] senthilkumarmca76@gmail.com, https://orcid.org/0000-0001-5131-7428

Abstract
Over the past few years, the devices in Wireless Sensor Networks (WSN) are growing exponentially due to the emergence of many sophisticated applications. This tremendous growth leads to serious security challenges, and the devices of WSN should be protected from various attacks. WSN can be configured dynamically without fixed infrastructure and the devices can be talked with one another in an ad-hoc manner. Due to the dynamic nature of WSN, routing is considered as the challenging task that should be performed efficiently with robust routing mechanism. Even though many routing schemes have been emerged for WSN, they are not well scalable in very large-scale environment. This work introduces multi path routing strategy, and the routing will be selected based on trusted nodes. First, the trusted nodes are identified using trusted metrics of each node in the network. These metrics are calculated based on the threshold value of nodes. Then, secure routing is established by isolating node capturing attacks from the path. The performance of the work is analyzed in terms of packet loss, computational time and throughput. The paper compares the performance with the state-of-the-art routing schemes such as EMBTR (Enhanced Multi Attribute Based Attack Resistance), TSRM (Trust based secure routing model), and TARF (Trust-aware routing framework for WSNs). The outcome of the simulation shows that the proposed scheme outperforms the other state-of-the-work in terms of computational cost, throughput, and delay.

Keywords
routing, security, node capturing, WSN

For citation: Kolangiappan J., Senthil Kumar A. A multi-path secure routing for the detection of node capturing attack in wireless sensor network. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 6, pp. 1127–1135. doi: 10.17586/2226-1494-2022-22-6-1127-1135

УДК 004.77

Многопутевая безопасная маршрутизация для обнаружения атаки с захватом узла в беспроводной сенсорной сети

Джаяраман Колангиаппан[1]✉, А. Сентил Кумар[2]

[1] Университет Перияр, Салем, 636011, Индия
[2] Аригнар Анна Говермент Артс Колледж, Намаккал, 637002, Индия

[1] jkakshiya@gmail.com✉, https://orcid.org/0000-0001-5093-5822
[2] senthilkumarmca76@gmail.com, https://orcid.org/0000-0001-5131-7428

Аннотация
За последние несколько лет количество устройств, используемых в беспроводных сенсорных сетях (Wireless Sensor Networks, WSN), растет в геометрической прогрессии. Данный рост связан с появлением множества сложных приложений, что приводит к серьезным проблемам безопасности. Устройства в WSN должны быть защищены от воздействия различных атак. Сети можно настроить динамически без фиксированной инфраструктуры, а их устройства могут обмениваться данными друг с другом в режиме ad-hoc. Из-за динамической природы WSN-маршрутизация считается сложной задачей, которая должна эффективно

выполняться с помощью надежного механизма. Несмотря на то, что для таких сетей разработано множество схем маршрутизации, они плохо масштабируются. В работе представлена стратегия многопутевой маршрутизации. Маршрутизация выбрана на основе доверенных узлов, которые идентифицированы с использованием доверенных показателей каждого узла в сети. Метрики рассчитаны на основе порогового значения узлов и далее установлена безопасная маршрутизация с помощью изоляции от пути узла, перехватывающего атаки. Выполнен анализ производительности работы сети с точки зрения потери пакетов, времени вычислений и пропускной способности. Приведено сравнение производительности с современными схемами маршрутизации, такими как расширенная устойчивость к атакам на основе нескольких атрибутов (Enhanced Multi Attribute Based Attack Resistance, EMBTR), модель безопасной маршрутизации на основе доверия (Trust based Secure Routing Model, TSRM) и инфраструктура маршрутизации с поддержкой доверия для WSN (Trust-Aware Routing Framework for WSNs, TARF). Результат моделирования показал, что предложенная схема превосходит другие варианты с точки зрения вычислительных затрат, пропускной способности и задержки.

Ключевые слова
маршрутизация, безопасность, захват узла, WSN

Ссылка для цитирования: Колангиаппан Д., Сентил Кумар А. Многопутевая безопасная маршрутизация для обнаружения атаки с захватом узла в беспроводной сенсорной сети // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 6. С. 1127–1135 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-6-1127-1135

Introduction

Wireless Sensor Network (WSN) is a type of wireless network where group of sensors are deployed in any environment to sense the surroundings. The sensed data will be transferred to the recipient through intermediate nodes or Base Station (BS). Since the sensors are deployed in any environment, many security violations are possible including physical attacks. The applications of WSN are emerged in many real time applications such as surveillance, health care, agriculture and many areas. Most of the applications of WSN carry user's private data that needs to be protected from the attackers. Therefore, security is crucial for WSN application to face the challenges in current and future applications. The main focus of the paper is secure routing because multiple hops are possible for the WSN data to reach its destination. If any of the nodes in the path is compromised, then the security of the entire network is questionable [1–3]. Many routing attacks are possible during the routing process. Some of the attacks are DoS, packet forwarding, selective packet, wormhole, black hole, node capturing attacks, and much more [4–6]. DoS attack will shut the service of the whole system by sending frequent number of packets in the intention of flooding the bandwidth. Selective forwarding attack will not let the specific sender to reach the destination just by drop the packets selectively. In general, there are two classifications of attacks: active attack and passive attack. During the execution of active attack, the attacker will put some efforts to harm the confidential data of the user. In case of passive attack, attacker will not harm the system; however they will just monitor the communication channel in order to steal the user's credentials. This work focuses on node capturing attack since this attack is the combination of active attack and passive attack that could harm the environment more than any other attacks. This attack is considered as the most catastrophic one because the node captured by the invader will steal the cryptographic information of the network and cause malicious function inside the network. Thus, the confidentiality and integrity of the system cannot be preserved. The invader can do variety of malfunction to damage the security of the system [7]. First, it turns a normal node into a malicious node. Then it will gradually increase the number of malicious nodes in the network. The security mechanism for the system is categorized as low level and high-level security mechanisms. Low level attacks depend on the lower layers of networks. Network layer and other low-level layers should be protected against attack such as jamming attack and DoS attack. Session hijacking, caching, spoofing replay attacks are some of the attacks of higher layers. Despite WSN is challenging to variety of attacks, routing attack should be prevented to safeguard the private data of the user. The architecture of WSN consists of entity such as user, internet, BS, and sensor nodes. The deployment of sensor nodes has done as cluster-based technique. User can request the data from the sensor through internet. Request and response will be transferred to the intended node through many intermediate nodes or BS. Here each node can act as both router and data collector. The primary security requirement to safeguard the sensors in WSN is to protect the communication channel. Since the deployment of sensors can be in anywhere environment, many attacks in the network are possible during the communication of cluster nodes. This work considers node capturing attack to protect the WSN environment from this attack. Many works have been evolved for the prevention of node capturing from WSN. During the execution of node capturing, the adversary will modify the sensitive details of the captured node and redeploy it to the network. This captured node will act as a regular node and communicate with the other nodes in the cluster. All the nodes in the cluster will share the confidential information such as cryptographic key and other shared keys without the knowledge of malicious node present in the network. The further section of the paper is divided to four parts. In the first part, the work discusses the literature of various related works for the detection of node capturing attack. Second part introduces the proposed work and the discussion about the novelty of how it differs from other works. In the third part, the results of the proposed work are discussed. Finally, the work is concluded.

Related works

There are various trust related schemes were employed in the previous works for the security of routing in WSN.

In [8], authors introduced a new approach called program integrity verification for the detection of node captured attack. The proposed technique is embedded in the access point of the cluster in order to safeguard the content of program memory. Additionally, the content of the data to be communicated is encrypted with hash-based encryption scheme in order to avoid any modification during transit. Authors claim that the proposed work can efficiently elude the node capture attack. However, the proposed method depends on the strong encryption scheme which makes the key generation process inefficient that leads to increased time complexity. Authors in [9] proposed a replica detection technique where they compared the earlier schemes for replica detection. The performances of the schemes are compared in terms of time, cost, energy, and packet delivery rate. The authors conclude that RED detection method achieves better detection rate among all the schemes. However, location dependent schemes are not efficient because it incurs memory overhead to save the location related information. Lin & Wu, 2016 [10], proposed a novel method for enhancing the efficiency of node capturing detection. First, authors developed a model to identify the unique behavior of node capturing attack. Then, they designed a countermeasure to defense against this attack. The proposed Matrix based model is well efficient in terms of detection rate and time. However, the computational complexity degrades the performance of the work that leads to increased energy. Authors in [11] discuss the importance of eluding node capturing in WSN environment. The authors proposed a multi factor authentication scheme for the prevention of node capturing attack. The researchers first investigated the signature of the attack and the capabilities of adversaries performing node capturing attack. The work also classified the different types of node capturing technique executed by the adversaries and modeled each type to find its nature. Even though, the suggested framework can be useful for creating secure path, the work increases the time complexity in processing multi factor authentication. In [12], authors proposed trusted routing schemes based on trusted metrics. The work computed the trusted value for each node in the network. Then the nodes are selected in the communication path based on the trusted value stored in a node. This value is calculated from the behavior of each node during the communication in the network. The performance of the work was analyzed in terms of node's reliability rate, stability rate, and elapsed time. Authors claimed that the work outperforms the other related works with their Quality of Service metrics. However, there is no proper evident shown in the work about the practical complexity in selecting the best route among all the possible trusted routes. Authors in [13] proposed an efficient security scheme for the isolation of blackhole, wormhole, and gray-hole attack with a single solution. In this work, trustworthy path can be established based on the capability-based model introduced here. However, it is unclear how efficiently the proposed model is in protecting against all three attacks in a single solution.

From the literature studies, we came to understanding that most of the current model focused on eliminating the attacks without properly investigating about the computational complexity in the detection process of their solutions. Each solution in the existing schemes is proportional to one another. We also learnt that creating trust relation between the nodes in the cluster make the routing process more secure. To make the detection process more efficient, we proposed a secure routing scheme with reduced energy, computational cost and delay.

The proposed secure routing scheme

The work proposed a trust based secure routing based on enhanced Ad-hoc On Demand Vector protocol. The main objective of the work is to elude node capturing with reduced time and cost. To achieve this, we use only few parameters for consideration during the computational work process. The main target of the attacker is network layer because this layer is responsible for addressing, and packet delivery. Many attacks are possible to redirect the packet into attacker's destination. To combat the node capturing efficiently and to provide a trusted route, the work introduces the detection methods such as taken based authentication, and threshold based trusted metrics.

Token based authentication

A token-based protocol is proposed for authentication of devices before they send data to other devices. A token is generated in a form of ticket which needs to be shown before accessing any device in the network. This token is created based on the information about the device such as device id, random key, and the access rights. If a device wants to communicate with other device in the cluster, both sender and receiver need to be mutually authenticated before start its transmission process. This protocol consists of two phases. In phase 1, token generation process takes place. In phase 2, application of AES_GCM based encryption is applied. The token will be generated based on the rights R_i, device identifier ID_i and Random number $RAND_i$. The random number used in the protocol is to protect the network from forgery. After the token is crated, it is hashed and encrypted with public key.

Fig. 1 shows the architecture of the proposed token-based scheme. If device A wants to connect with device B, it will send the token to device B. The token consist of details such as device identifier ID_i, Rights that the device possess to access a resource '*r*' are hashed and encrypted with encryption key E_k using AES algorithm. After receiving the token from device A, device B will decrypt the token using public key which is made available publicly in the cluster. Then it will check the hash function for any modification. If the token is valid, then device A will be allowed to access device B. Similarly, device B will initiate the same process for verification. In this way both devices are mutually authenticated. For the encryption of token, AES_GCM based algorithm is used in the work. This algorithm supports both authentication and confidentiality.

The input of the algorithm is Starting Variable for generating pseudo random number, public key to be used for encryption, plain text and authentication field. The output of the algorithm is encrypted text. Starting Variable can be generated by a device during communication process to perform authenticated encryption. Authentication file is used to authenticate the address of the sender and receiver.

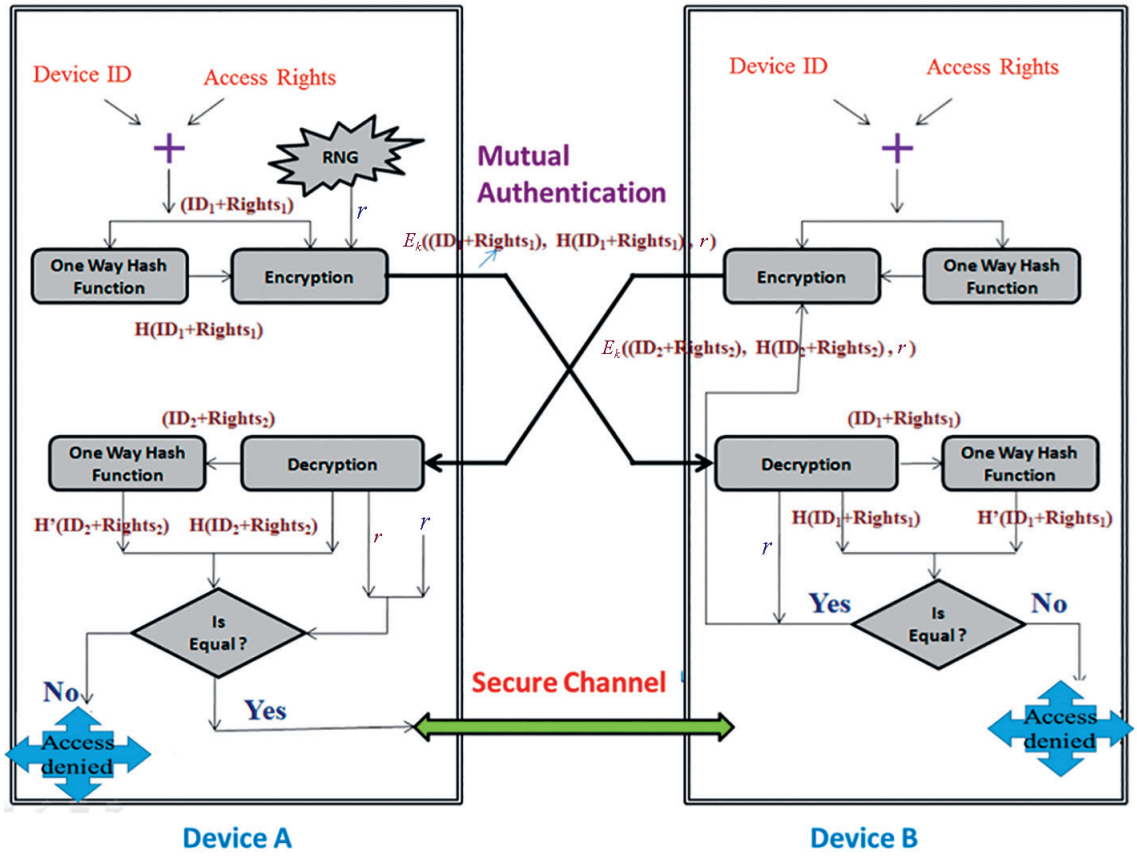

Fig. 1. The proposed Architecture

The token-based authentication protocol is designed based on the delegation model which consists of three devices such as Sensor device, Coordinator, and Gateway device. Coordinator node acts as a key distribution device, it establishes a secret key, then shares it with the other two devices such as Sensor node and the gateway node. There is an assumption that the Sensor and the Coordinator have a pre-established trust relationship and they share symmetric key K_S but the devices don't have direct communication. However, there is direct communication possible for the gateway device with both the Sensor and the Coordinator. The result of this protocol is a symmetric key to be shared between gateway and sensor.

The Sensor, the Gateway, and the coordinator are denoted by *S*, *G* and *C* respectively in the following discussion.

The steps involved in the protocol specifications is given below:

1. $G \rightarrow S$: {Nonce$_i$, ID$_i$}
   The protocol session is initiated by the gateway node by sending a message 1 to Sensor node *S*. The trust relationship is established by sharing a symmetric key K_S. *G* sends this message to *S* by generating Noncei with its identifier ID$_i$ and send it to *S* in cleartext.
2. $S \rightarrow G$: {Nonce$_i$, ID$_i$, Nonce$_j$, ID$_S$, ID$_C$}
   Sensor node *S* will not have any knowledge about gateway node *G*. However, it sends message 2 to Coordinator *C* to perform authentication and delegation. This message consists of information about all the three entities, *S*, *C*, and *G*, and nonce values from *S* and *G*.
3. $G \rightarrow C$: {Nonce$_i$, ID$_i$, Nonce$_j$, ID$_S$, ID$_C$}
   After the message 2 is received, *G* first verifies the message 1 with its Noncej and ID$_G$. It ensures duplicate identification has not occurred, i.e., ID$_S$, ID$_G$ and ID$_C$, ID$_G$ and ID$_S$, ID$_C$. After the successful verification, the gateway node *G* will forward message 3 to the coordinator node of *S*.
4. $C \rightarrow G$: {Nonce$_i$, ID$_G$, Nonce$_j$, ID$_S$, ID$_C$, Nonce$_k$, g^x}
   When message 3 is received, *C* has to perform the following verification:
   — Check the identification information received.
   — Authenticate *G*.
   — Sensor node S_i is fixed.
   — *G*'s request for access on *S* can be granted.
   — Authentication and authorization are based on *G*'s identity. Authorization can be done with additional information required in different situations. In that case, data can be validated by *C* and *G* through protocol exchange with the help of message 4, 5 and 6.

   Later Nonce$_3$ can be established by *S*, D-H-key K_x and the data g^x to build message 4, which is similar to message 1 of SIGMA protocol.

   The message generated here will comprise all the nonce Nonce$_i$ in order to improve the three way communication. The gateway node *G* will prevent the chance of a DoS attack on *C*.

5. $G \rightarrow C$: {Nonce_1, Nonce_2, Nonce_3, g^y, S_G ($g^x||g^y$), [ID_S, PUK_G]K_S}

   Here messages 4, 5 and 6 are used to authenticate *C* and *G* mutually. Initially *G* performs authentication by verifying nonce values and the value g_x received from message 3. Then message 5 is sent from the gateway node *G*, which is related to the SIGMA protocol in message 2, then MAC value is computed based on identity of *G*, nonce values, identifiers using its public key certificate PUK_G.

   The key K_S can be obtained from the equations:

$$K_d = f(h(\text{Nonce}_1||\text{Nonce}_2||\text{Nonce}_3), g^{x,y}), \quad (1)$$

$$K_s = f(K_s, 1). \quad (2)$$

   In the above equations (1) and (2), K_d and K_s are the decryption keys of any symmetric key, respectively. $f(h)$ represents the hash function to be generated. $g^{x,y}$ represent the data generated by gateway node for device *X* and device *Y*.

6. $C \rightarrow G$: {a, b, $S_c(g^y||g^x)$, [PUK_C]K_S}

   The following verifications are done by *C*

   — All the nonce values, PUK_G, and ID_S verified against message 4.
   — PUK_G is verified and authorize *G* for a key to be received by *S*.
   — The signature in the PUK_G SG ($g^x||g^y$) is verified.
   — The public value g_y is verified.
   — K_S is used to verify the MAC on [ID_S, PUK_G]K_S.

   In the above step, g^x, g^y are the data generated by gateway node for device *X* and device *Y*, K_x is the exchange of secret key and K_x is the symmetric key.

Threshold based resistance to node capturing

The threshold-based protocol is also introduced in the work to elude the node capturing from the route. The type of attack that we consider for evaluation is node capturing attack. It is assumed that all the nodes in the WSN are randomly distributed in the cluster, and communication can take place in both single hop and multi hop [14–16]. Behavior of each node is identified and a threshold value is fixed for each node in the network and the details are stored in BS based on their activities. This threshold value is fixed for a node from its sending behavior in a particular time gap. If any node exceeds the threshold, then it is identified as suspicious node. Then the algorithm will compute route analysis. During this analysis, the algorithm will check the distance of the suspicious node. If the distance of the node is in one hop, then it is possible to detect the attack easily [17–20]. If the node is in multi hop distance, then it will check all the nodes in the network in route analysis process. If it is confirmed that the node sends more than allowed, then the node is considered as malicious node and it will be removed from the network. The main characteristics of the proposed work, its advantages and disadvantages are given in Table 1.

Results and discussion

The implementation of the proposed work is simulated in real time scenario. The simulation parameter is shown in Table 2. The performance of the work is evaluated in terms of energy, delay, and throughput under 2 different conditions.

1) WSN with node capturing under normal condition
2) WSN with node capturing under Mountain Safety Research (MSR), Trust-Aware Routing Framework for WSNs (TARF), Trust based Secure Routing Model (TSRM), and Enhanced Multi Attribute Based Attack Resistance (EMBTR).

There are two sets of simulation performed to evaluate the performance of the proposed work. In the first set, we did the evaluation under traffic intervals. The time of the interval is specified from 1s to 10s. Traffic interval under 1s is considered as fast and 10s is considered as slow.

Performance analysis under traffic interval in terms of energy, delay, and throughput

Fig. 2 shows the results of the work by considering energy, delay, and throughput under traffic interval from 1s to 10s. From the results, we observed that the proposed MSR enhances the energy, delay, and throughput by analyzing the network traffic and isolate the node capturing attempt. The important reason for the improved energy is that the MSR detects the node which performs node capturing and removes it from the network. Thereby saves the energy that may rise because of that malicious node. The reason for minimum delay is that the work can effectively detect the attack and isolate it from the network that gives the way for other nodes to continue their work without extra delay. Execution of this attack in one node can spread the same to many nodes in the network which will make the other nodes to wait for accessing the channel long time. After applying MSR, throughput is improved by reducing the waiting time of the nodes in the network under without attack condition.

Table 1. Summary of proposed work

Characteristics	Advantages	Disadvantages
Key pre distribution	Combination of secret key and public key	Sharing of key
Shared key discovery	Secured communication path through pair wise key	Broadcasting of messages related to shared key
Authenticated encryption	Supports both authentication and encryption	Software implementation is complex
Threshold based countermeasure	Easily detect the attacker node based on the threshold value stored in each node	Path analysis in multi hop network is difficult

Table 2. Simulation parameters

Parameter	Setting
Interface	Wireless channel
Antenna	Omni direction
Access control	MAC80.2.15.4
Routing	Ad-hoc on demand
Number of nodes	50
Power, mW	35
Energy level, J	100

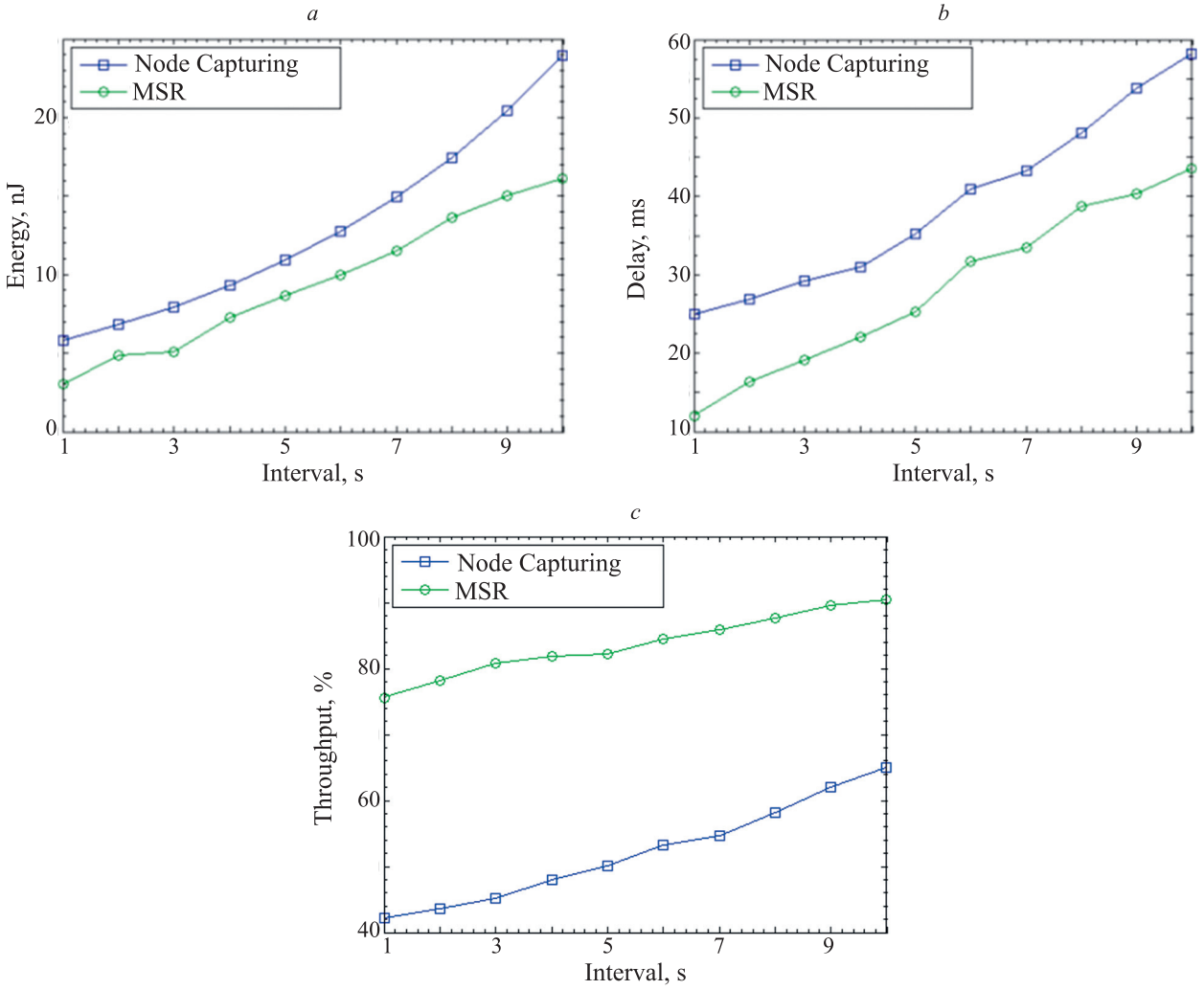

Fig. 2. Energy analysis (*a*), delay analysis (*b*) and throughput (*c*) in the interval of traffic with attack and MSR

Performance analysis with increased attacker nodes

Fig. 3 shows the outcome of the work by considering energy, delay, and throughput under increased malicious nodes. From the graph, we observed that the performance of the network has been significantly improved after applying MSR. This improvement is due to the efficient mechanism of the proposed work in defensing the attack. The proposed work is effective against increased malicious nodes in the network by detecting multiple attacks that happened in the network. The work achieves reduced energy than the other schemes such as TARF, TSRM, and EMBTR due to the removal of node capturing attacks by considering only trusted nodes in the network. The algorithm will select the trusted path based on the trusted metrics calculated for each node. All the trusted nodes in the network are selected as a route for data transmission which leads to reduction in energy. The work achieves better delay and throughput than the other schemes because of the reduction in waiting time and the response in sensing for node availability.

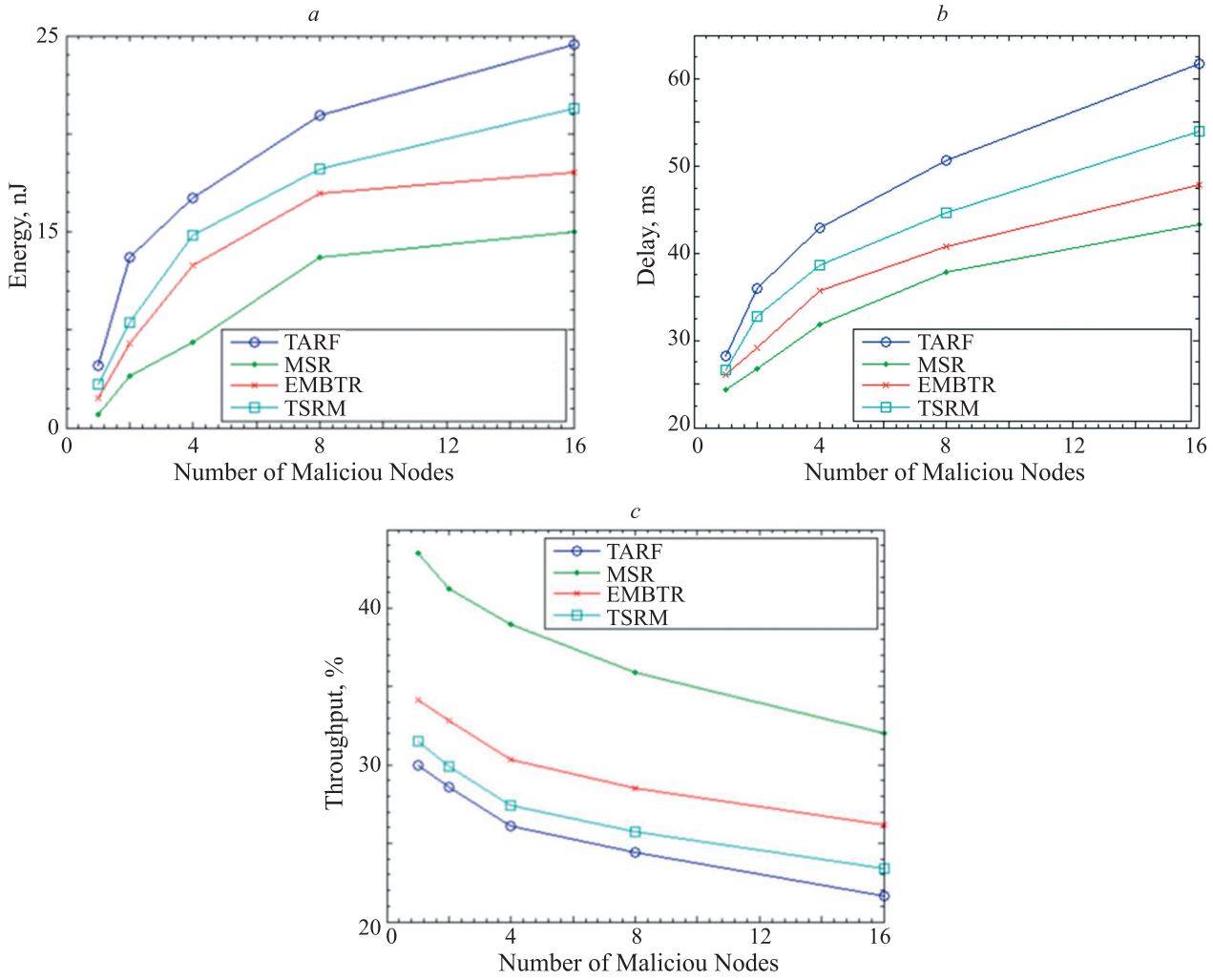

Fig. 3. Energy analysis (*a*), latency (*b*) and throughput (*c*) analyzes with increased number of malicious nodes

Conclusion

The work presents a multi path secure routing scheme MSR. Since the WSN nodes can be deployed in any environment such as military, hospital, banking and many more areas, there should be a strong security mechanism to protect the sensitive data. In our proposed work, a secure channel based on trusted nodes can be established for the transmission of data. Each node should possess a token for authentication before accessing any device. Only trusted nodes are participated during the communication process. This trusted node is identified based on the threshold value stored on each node in the network. Threshold value is the average number of data sent and received for a particular node. The nodes can be in three states, such as normal state, suspicious state, and attack state, to identify the attack. If any of the nodes is confirmed as attacker node based on the trusted metrics, then it is removed from the network. The novelty of the work is its multi hop path analysis process which takes place once the suspicious node is confirmed. The performance of the work is compared with other works such as TARF, TSRM, and EMBTR. Simulation results prove the reliability of the proposed MSR scheme. According to the results obtained in the work, the model is proposed in terms of energy, delay, packet delivery rate, and false node detection rate. In future, we plan to investigate our work on different types of jamming attacks.

References

1. Albakri A., Harn L. Non-Interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks. *IEEE Access*, 2019, vol. 7, pp. 31615–31623. https://doi.org/10.1109/ACCESS.2019.2900390
2. Airehrour D., Gutierrez J.A., Ray S.K. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Generation Computer Systems*, 2019, vol. 93, pp. 860–876. https://doi.org/10.1016/j.future.2018.03.021

Литература

1. Albakri A., Harn L. Non-Interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks // IEEE Access. 2019. V. 7. P. 31615–31623. https://doi.org/10.1109/ACCESS.2019.2900390
2. Airehrour D., Gutierrez J.A., Ray S.K. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things // Future Generation Computer Systems. 2019. V. 93. P. 860–876. https://doi.org/10.1016/j.future.2018.03.021

3. Ali R., Pal A.K., Kumari S., Karuppiah M., Conti M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Generation Computer Systems*, 2018, vol. 84, pp. 200–215. https://doi.org/10.1016/j.future.2017.06.018
4. Han L., Zhou M., Jia W., Dalil Z., Xu X. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. *Information Sciences*, 2019, vol. 476, pp. 491–504. https://doi.org/10.1016/j.ins.2018.06.017
5. Shajilin Loret J.B., Vijayalakshmi K. Security enrichment with trust multipath routing and key management approach in WMN. *IETE Journal of Research*, 2018, vol. 64, no. 5, pp. 709–721. https://doi.org/10.1080/03772063.2017.1369365
6. Usman A.B., Gutierrez J. DATM: A dynamic attribute trust model for efficient collaborative routing. *Annals of Operations Research*, 2019, vol. 277, no. 2, pp. 293–310. https://doi.org/10.1007/s10479-018-2864-5
7. Zawaideh F., Salamah M. An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems*, 2019, vol. 32, no. 3, pp. e3878. https://doi.org/10.1002/dac.3878
8. Agrawal S., Das M.L., Lopez J. Detection of node capture attack in wireless sensor networks. *IEEE Systems Journal*, 2019, vol. 13, no. 1, pp. 238–247. https://doi.org/10.1109/JSYST.2018.2863229
9. Mishra A.K., Turuk A.K. A comparative analysis of node replica detection schemes in wireless sensor networks. *Journal of Network and Computer Applications*, 2016, vol. 61, pp. 21–32. https://doi.org/10.1016/j.jnca.2015.12.001
10. Lin C., Wu G. Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. *Journal of Supercomputing*, 2013, vol. 66, no. 2, pp. 989–1007. https://doi.org/10.1007/s11227-013-0965-0
11. Wang C., Wang D., Tu Y., Xu G., Wang H. Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing*, 2022, vol. 19, no. 1, pp. 507–523. https://doi.org/10.1109/TDSC.2020.2974220
12. Khan F.A.B., Hannah L., Devi K.S., Rajalakshmi S. A multi-attribute based trusted routing for embedded devices in MANET-IoT. *Microprocessors and Microsystems*, 2022, vol. 89, pp. 10446. https://doi.org/10.1016/j.micpro.2022.104446
13. Vidhya Lakshmi G., Vaishnavi P. An efficient security framework for trusted and secure routing in MANET: A comprehensive solution. *Wireless Personal Communications*, 2022, vol. 124, no. 1, pp. 333–348. https://doi.org/10.1007/s11277-021-09359-2
14. Nikokheslat H.D., Ghaffari A. Protocol for controlling congestion in wireless sensor networks. *Wireless Personal Communications*, 2017, vol. 95, no. 3, pp. 3233–3251. https://doi.org/10.1007/s11277-017-3992-y
15. Jin X., Liang J., Tong W., Lu L., Li Z. Multi-agent trust-based intrusion detection scheme for wireless sensor networks. *Computers and Electrical Engineering*, 2017, vol. 59, pp. 262–273. https://doi.org/10.1016/j.compeleceng.2017.04.013
16. Wu F., Xu L., Kumari S., Li X. A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer-to-Peer Networking and Applications*, 2017, vol. 10, no. 1, pp. 16–30. https://doi.org/10.1007/s12083-015-0404-5
17. Shin S., Kwon T., Jo G.-Y., Park Y., Rhy H. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *IEEE Transactions on Industrial Informatics*, 2010, vol. 6, no. 4, pp. 744–757. https://doi.org/10.1109/TII.2010.2051556
18. Ayday E., Fekri F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks. *IEEE Transactions on Mobile Computing*, 2012, vol. 11, no. 9, pp. 1514–1531. https://doi.org/10.1109/TMC.2011.160
19. Kamvar S., Schlosser M., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. *Proc. of the 12th International Conference on World Wide Web*, 2003, pp. 640–651. https://doi.org/10.1145/775152.775242
20. Umar I.A., Hanapi Z.M., Sali A., Zulkarnain Z.A. TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks. *IEEE Access*, 2017, vol. 5, pp. 2550–2562. https://doi.org/10.1109/ACCESS.2017.2672827

3. Ali R., Pal A.K., Kumari S., Karuppiah M., Conti M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring // Future Generation Computer Systems. 2018. V. 84. P. 200–215. https://doi.org/10.1016/j.future.2017.06.018
4. Han L., Zhou M., Jia W., Dalil Z., Xu X. Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model // Information Sciences. 2019. V. 476. P. 491–504. https://doi.org/10.1016/j.ins.2018.06.017
5. Shajilin Loret J.B., Vijayalakshmi K. Security enrichment with trust multipath routing and key management approach in WMN // IETE Journal of Research. 2018. V. 64. N 5. P. 709–721. https://doi.org/10.1080/03772063.2017.1369365
6. Usman A.B., Gutierrez J. DATM: A dynamic attribute trust model for efficient collaborative routing // Annals of Operations Research. 2019. V. 277. N 2. P. 293–310. https://doi.org/10.1007/s10479-018-2864-5
7. Zawaideh F., Salamah M. An efficient weighted trust-based malicious node detection scheme for wireless sensor networks // International Journal of Communication Systems. 2019. V. 32. N 3. P. e3878. https://doi.org/10.1002/dac.3878
8. Agrawal S., Das M.L., Lopez J. Detection of node capture attack in wireless sensor networks // IEEE Systems Journal. 2019. V. 13. N 1. P. 238–247. https://doi.org/10.1109/JSYST.2018.2863229
9. Mishra A.K., Turuk A.K. A comparative analysis of node replica detection schemes in wireless sensor networks // Journal of Network and Computer Applications. 2016. V. 61. P. 21–32. https://doi.org/10.1016/j.jnca.2015.12.001
10. Lin C., Wu G. Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach // Journal of Supercomputing. 2013. V. 66. N 2. P. 989–1007. https://doi.org/10.1007/s11227-013-0965-0
11. Wang C., Wang D., Tu Y., Xu G., Wang H. Understanding node capture attacks in user authentication schemes for wireless sensor networks // IEEE Transactions on Dependable and Secure Computing. 2022. V. 19. N 1. P. 507–523. https://doi.org/10.1109/TDSC.2020.2974220
12. Khan F.A.B., Hannah L., Devi K.S., Rajalakshmi S. A multi-attribute based trusted routing for embedded devices in MANET-IoT // Microprocessors and Microsystems. 2022. V. 89. P. 10446. https://doi.org/10.1016/j.micpro.2022.104446
13. Vidhya Lakshmi G., Vaishnavi P. An efficient security framework for trusted and secure routing in MANET: A comprehensive solution // Wireless Personal Communications. 2022. V. 124. N 1. P. 333–348. https://doi.org/10.1007/s11277-021-09359-2
14. Nikokheslat H.D., Ghaffari A. Protocol for controlling congestion in wireless sensor networks // Wireless Personal Communications. 2017. V. 95. N 3. P. 3233–3251. https://doi.org/10.1007/s11277-017-3992-y
15. Jin X., Liang J., Tong W., Lu L., Li Z. Multi-agent trust-based intrusion detection scheme for wireless sensor networks // Computers and Electrical Engineering. 2017. V. 59. P. 262–273. https://doi.org/10.1016/j.compeleceng.2017.04.013
16. Wu F., Xu L., Kumari S., Li X. A new and secure authentication scheme for wireless sensor networks with formal proof // Peer-to-Peer Networking and Applications. 2017. V. 10. N 1. P. 16–30. https://doi.org/10.1007/s12083-015-0404-5
17. Shin S., Kwon T., Jo G.-Y., Park Y., Rhy H. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks // IEEE Transactions on Industrial Informatics. 2010. V. 6. N 4. P. 744–757. https://doi.org/10.1109/TII.2010.2051556
18. Ayday E., Fekri F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks // IEEE Transactions on Mobile Computing. 2012. V. 11. N 9. P. 1514–1531. https://doi.org/10.1109/TMC.2011.160
19. Kamvar S., Schlosser M., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks // Proc. of the 12th International Conference on World Wide Web. 2003. P. 640–651. https://doi.org/10.1145/775152.775242
20. Umar I.A., Hanapi Z.M., Sali A., Zulkarnain Z.A. TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks // IEEE Access. 2017. V. 5. P. 2550–2562. https://doi.org/10.1109/ACCESS.2017.2672827

Authors

Jayaraman Kolangiappan — PhD, Research Scholar, Periyar University, Salem, 636011, India, https://orcid.org/0000-0001-5093-5822, jkakshiya@gmail.com
Angamuthu Senthil Kumar — PhD, Assistant Professor, Arignar Anna Government Arts College, Namakkal, 637002, India, SC 57196435711, https://orcid.org/0000-0001-5131-7428, senthilkumarmca76@gmail.com

Авторы

Колангиаппан Джаяраман — PhD, исследователь, Университет Перияр, Салем, 636011, Индия, https://orcid.org/0000-0001-5093-5822, jkakshiya@gmail.com
Сентил Кумар Ангамуту — PhD, доцент, Аригнар Анна Говермент Артс Колледж, Намаккал, 637002, Индия, SC 57196435711, https://orcid.org/0000-0001-5131-7428, senthilkumarmca76@gmail.com

Received 15.06.2022
Approved after reviewing 27.09.2022
Accepted 09.11.2022

Статья поступила в редакцию 15.06.2022
Одобрена после рецензирования 27.09.2022
Принята к печати 09.11.2022