IJCSMA

Ahmed Kreem Aljabery *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 8, August- 2022, pg. 80-92 **ISSN: 2321-8363**
Impact Factor: 6.308

(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

DYNAMIC ROUTING FOR MULTI-HOP WIRELESS NETWORK

Ahmed Kreem Aljabery[1]; Maha Ali Hussein[2]; Abdulhakeem Amer Abdulameer[3]

[1] ahmed.ahmed8430@yahoo.com
[2] maha_2016@uomustansiriyah.edu.iq
[3] abdulhakeem@nahrainuniv.edu.iq

DOI: 10.5281/zenodo.7107957

ABSTRACT

To run wireless nodes capable of data transmission over a wireless connection. Consequently, selecting the optimal paths between both the network entities are challenging, and this network type is known as a multi-hop wireless network (MHWN). Many researchers have been researching this problem and have offered routing protocols to aid nodes in discovering optimal multi-hop routes. The military, the healthcare industry, and national security are just a few sectors that benefit from multi-hop wireless networks. The data transmission needs of such applications are severe and crucial, necessitating a specific level of accuracy and security. Since the devices in a multi-hop network have fewer resources like memory and power, securing data transmission is complex. Here, we offer a safe and efficient routing protocol. Choosing a safe route between the source and the destination is crucial to this concept since it will increase the network's performance and security. We propose generating a standard key between the data's origin and destination to secure the data's transport. We offer considering the power of the intermediary nodes along the chosen route, as the devices need limited energy. Extensive simulations are done in the Network Simulator to examine the effectiveness of the suggested protocol. Edge latency, overhead, and infected device counts are examined considering Secured Ad-Hoc On-Demand Route Discovery (SAHODV).

KEYWORDS: Network Simulator, Secure Route, Multi-Hop Wireless Network, Routing Protocol, Packets.

This work is licensed under a Creative Commons Attribution 4.0 International License.

INTRODUCTION

Multi-hop Wireless Networks (MHWNs)[1], that concern sensor technology, mobile ad - hoc networking, as well as the Internet of Things (IoT)[2], consist of autonomous nodes that communicate with one another wireless data and independently, eliminating the need for a hub or multiple hubs [3]. These networks are referred to as MHWNs. Because of this, the primary responsibility of such a network is to transmit data from one node to another for the data to arrive at its final location. Because of this, the network nodes must communicate to share route information. It is a fundamental issue, and as a result, many academics are working on the development of routing protocols[4] that will make it possible for devices to find a multi-hop path between one other. Reactive protocols, proactive protocols, and hybrid routing protocols are the three different categories of routing protocols.

Each node participating in the proactive protocol is responsible for maintaining a routing table containing information about the currently used paths. If the routing database includes a path leading to the destination, the sending node will take that path if available. Among the proactive routing systems that have been developed are the Destination Sequence Distance Vector (DSDV), Optimized Link State Routing Protocol (OLSR), and the Wireless Routing Protocol (WRP), to name just a few. To reduce the amount of work that must be done by the network, reactive systems such as Temporarily Ordered Routing Protocol (TORA), Dynamic Source Routing (DSR), and Ad-hoc On-Demand Distance Vector (AODV) need to have only one active route. The hybrid protocol incorporates aspects of both reactive and proactive strategies to produce a plan that is more all-encompassing[5] [6] [7] [8] [9] [10] .

The inherently unstable topology, poor energy efficiency, and high mobility of multi-hop wireless networks all present potential roadblocks to the capacity of these networks to support a diverse set of application use cases. Because of this, these difficulties should be considered when expanding the capabilities of MHWN, such as the multi-hop routing protocols and designing new ones.

It is vital to consider the nodes' involvement in the routing process while building a routing protocol for MHWN[11]. It is because the nodes are what perform the routing. It makes security an extra essential factor to consider. During the process of route discovery, an adversary can join the route that has been chosen and then execute additional assaults, such as dropping packets, creating forged packets, or injecting malicious code. Because of the required calculation, including security in multi-hop routing systems results in increased storage space consumption and other resources. It is not ideal in the MHWN because of the constrained nature of the node resources. When assuring the routing in MHWN, it is necessary to ensure the optimal use of resources, most notably the help that deals with energy.

This work is licensed under a Creative Commons Attribution 4.0 International License.

On the other hand, a significant number of the proposed protocols view the problems of resource efficiency and security as two independent issues.

Security measures included in routing algorithms must protect data as it moves from a source address to the goal. Most of the suggested protocols ensure that nearby nodes do not divulge private information, protecting users' privacy. In order to accommodate a growing network, it has been proposed that perhaps the number of public keys should also grow. It leads to excessively high consumption of resources, which is especially problematic in virtual networks such as sensor networks, where individual sensor nodes have limited resources.

Within the confines of this investigation, we will provide an innovative multi-hop routing technique for the MHWN. This technique takes security seriously by utilizing the most foolproof and covert methods available to guarantee authentication, data privacy, and data integrity. To protect the privacy of individuals whose information is being transmitted, our team suggests assigning a one-time-only, one-of-a-kind identity to each node taking part in the process. that will ensure that no personal details are revealed. This technique considers the amount of remaining battery life possessed by the selected nodes to achieve such network performance levels. It is correct that the high-energy hubs can be chosen as potential destinations throughout the path-finding procedure. When a target receives a large number of request packets, it uses a specified cost function to select between lifetime routes with the short and longest periods of operation in order to execute the requests in the shortest possible time frame.

REVIEW OF LITERATURE

Numerous routing strategies have been created and published in the scientific literature to enhance the operational capabilities of MHWNs. A proposal was made for a multi-hop routing system for the Internet of Things that uses a virtual cellular grid[12]. This proposal aims to establish a more even distribution of energy consumption across the system to increase the network's lifespan. It will be accomplished by creating a more even distribution of energy consumption. When calculating how much it will cost to go from the source node to the destination node, it is necessary to consider the amount of energy spared and the physical distance separating the two nodes. O. Salwa and colleagues have suggested utilizing an on-demand routing method in multi-hop mobile networks that is based on fuzzy logic. [13]. This system was developed for use in multi-hop cellular networks. Using a method based on fuzzy logic, the authors integrate three different indicators to achieve the best possible performance from the network. The Signal Interference and Noise Ratio (SINR), The three measures used in this context are the Gain Time, the Remaining Energy, and both. A multi-hop networking architecture with reduced overhead is suggested as a remedy for equipment communication in 5G networks[14][15]. The DSR protocol

This work is licensed under a Creative Commons Attribution 4.0 International License.

is utilized in the suggested solution to facilitate a speedy determination of the 5G network topology that is most suitable. Reducing the number of control signals transmitted is feasible to save time and energy during route finding. It will, in turn, result in fewer errors. When these three protocols are used, there is an increase not only in the energy efficiency of the networks but also in the longevity of the networks. The most significant problem with these recommendations is that they do not adequately address concerns over safety.

The multi-hop network routing technology will be protected and improved by implementing additional scheduled improvements. H. Kojima and colleagues proposed protecting the DSR protocol by signing the routing data using a sequential aggregate signature[16]. It would prevent unauthorized access to the routing information. Devices cannot communicate with one another if this idea is implemented since it requires them to first generate and distribute keys from a centralized point. Consequently, a new device cannot connect to the network until this hub has validated it. In a routing protocol that they dubbed Expiration Time based Routing Protocol[17]. This protocol makes use of a one-time signature method. Before delivering any packet, each node performs a greedy calculation to determine the link timeout using the available information. The amount of data that can be moved over a network in a single packet is directly related to the rate at which data can be transferred across the web. When it comes to the process of routing data across MANETs, A. Bhusari et al. provide an approach that is both enhanced and safeguarded. This work had as its primary objective the reduction of the protocol's overhead and delay to make it more efficient. To protect our suggested protocol from multiple threats, A new metric based on a multi architecture is what we recommend. To ensure that the demand phase is properly protected, the intermediate node checks the RREQ using the group identities that it has got from its private key. The receiving node unlocks the data that has been supplied to it using the public key agreement key. This key was created by the sender node.

On the other hand, if the created signature were to be made public, it would put the integrity of the entire network at risk. It occurs because of the network nodes using the same key to share data.

A. Vinitha and colleagues proposed a safe multi-hop routing system that may be implemented in wireless sensor networks[18]. The trust model used by the study's authors contained an integrating factor, forward rate components, indirect trust, and direct confidence. It was carried out to ensure that customers wouldn't be in danger because of using the suggested approach. The trust elements are combined with various other considerations, including delay, distance, energy, interpersonal and inter distance, and inter-cluster distance, to carry out the proposal effectively. It is done to ensure that the suggestion is carried out. It is required to first design the network into its numerous clusters before continuing to select the

This work is licensed under a Creative Commons Attribution 4.0 International License.

most efficient route through the web. A methodology referred to as Low-Energy Adaptive Clustering Hierarchy (LEACH) is used to choose the leaders of the individual clusters[19].

K. Hamouid and colleagues presented a secure routing system that is built on trees for WSNs, also known as wireless sensor networks. Among the many types of cryptographic protocols, key agreement protocols are the most fundamental and ubiquitous. To accomplish their cryptographic goals, two or more people can utilize a key agreement mechanism to agree on a shared key. Furthermore, an authentication system guarantees that only authorized parties have access to the shared key. A protocol that can do both of these things is known as an Authenticated Key Agreement (AKA) protocol. The authors make use of a technique called as ID-Based AKA protocols in order to guarantee that the data that is being passed along from one node to another has not been altered in any way while it is in transit [20]. The suggested methodology provides authenticity and confidentiality at a price manageable for most people. Each node within the network owns its private key, which it utilizes to generate shared keys for the other nodes in its local proximity. In addition, to cut down on the amount of extra work produced by connectivity, each node sends out a short statement for both the growth of the routing tree and the establishment of the key. However, more complex activities must be carried out at each node to produce security keys using this protocol. Because of this, there is potential for an increase in the amount of power consumed by nodes.

Secure Ad Hoc On-Demand Distance Vector (SAHODV) is a protocol presented by Zapata et al. a custom layout of the AODV routing protocol has been developed that safeguards its security by ensuring the protocol's authenticity, integrity, and non-repudiation. SAHODV is an acronym for Secure Ad Hoc On-Demand Distance Vector[21]. The origin node and the destination node will need to append signatures generated with their private keys for the authentication to be completed successfully[22]. The intermediate nodes are not responsible for any mutual authentication; all they do is check the validity of the created signature. However, a hash chain is used so that the hop-count field may be relied upon to provide accurate information. In the box labelled "hash function"[23], we record the algorithm's name utilized to produce the hash result. Although several precautions are in place to secure the route request phase of the SAHODV protocol, it is nevertheless susceptible to a wide range of threats from various distinct attack vectors. It is because nodes that are physically close together are not authenticating their connections with one another. If both parties utilize the same hash value, the adversary can take part in the given route even though the hop-count field remains unaltered.

As a result of this, the legitimate nodes are unable to identify the assault that is being launched against them. The routing protocol created by M. Surajuddin and his colleagues and published has several purposes, including decreasing packet loss, and congestion, identifying malicious nodes, and transporting data safely. It is accurate that the originator sends out RREQ

This work is licensed under a Creative Commons Attribution 4.0 International License.

packets with a sequence number and destination address that have been faked[24]. A hacker is the only one who would respond with an RREP packet. When the IP address of an attacker is identified, the source adds it to the "blacklist" as well as notifies some other network components of the situation. Then again, a node's trust value is defined by how the node's neighbors feel about it. It is because neighbors are connected through the network. If the trust value of a node is lower than a predetermined threshold, then that node is dangerous for as long as the predetermined threshold is either met or exceeded. Impersonation and Sybil assaults, on the other hand, are not covered by the system in its current incarnation because of how it was constructed[25]. Consequently, these types of attacks are not protected.

In this section, we will discuss a new protocol we plan to implement to address the shortcomings of earlier works. Some of these shortcomings include an inability to authenticate across neighbouring nodes and the difficulty of computing a shared key. These issues can be remedied by implementing our new protocol.

SECURITY ANALYSIS

We analyze the plan's adherence to security limitations to show that it is safe despite the numerous dangers that could potentially occur it[26].

1. **Confidentiality**: The suggested technique encrypts the messages sent and received during requests and replies to phases by employing a secret key distributed among all nearby devices. For attackers to successfully compromise these keys, they will need to solve the PDLP, which is a challenging problem. It's just because they'll need to be aware of the obscure conditions required to generate each key. The phase of the information transmission that is being protected utilizes the shared key that is present between the origin and the destination of the data transfer. If the attacker wishes to steal this key effectively, they will first need to figure out how to circumvent the Asymmetric cryptographic challenge. As a result, the suggested protocol protects the confidentiality of the transmitted data.
2. **Authentication**: The proposed protocol mandates that each pair of neighbors exchange a secret key under the Weil Pairing method. By using this method, two people can communicate with one another while simultaneously validating the identity of the other using a standard set of secret parameters. Because it is based on the TP's private key, only authorized devices can generate this key and distribute it to their neighbors. A secret key is generated by each device and then shared with its neighbors. Additionally, the Asymmetric cryptographic problem is utilized to

This work is licensed under a Creative Commons Attribution 4.0 International License.

create a public key that is then applied in the authentication process between the origin and the destination. This shared key is used to verify the authenticity of the source. This key is employed to authenticate users before they may proceed. Authentication is consequently accomplished by utilizing the proposed protocol.

3. **Integrity**: According to the proposal, the MAC function will be included in every message transmitted to allow the sender to check the integrity of the message before sending it. To falsify the packet's innocence, an attacker would need to decrypt the packet and recompute the MAC function of the tampered package. However, the attacker can't do that because they don't have the secret key to decode the data message.
4. **Sybil Attack**: The intruder is said to have committed a Sybil attack when they established neighbor associations with other real devices while utilizing phony identities. When using a fake identity, an attacker cannot complete mutual authentication with a simple device since the attacker does not have a valid key that the TP provided. It is hard for an adversary to generate its private key to carry out a Sybil assault since it is challenging to solve the PDLP problem while at the same time retaining the trust party's private key. Given this, there is no risk of a Sybil attack being launched against the proposal.
5. **Replay Attack**: The hacker is transmitting many genuine packets repeatedly to fool the system into thinking they came from a different source. The protocol design includes several safeguards that render it immune to an attack of this kind. To begin, each freshly formed request packet from the source includes an identifier. Secondly, each device's secret key is calculated using the timestamp provided by the source. In addition, the shared keys for each session are derived from a brand-new random number produced by authorized devices. This number has no relevance to the values generated in any of the sessions that came before it. Because of this, the suggested protocol is protected from being subjected to a replay attack.
6. **Impersonation Attack**: An imitation assault is when the attacker appears as a trusted node to compromise the network by acting as a neighbor or taking the chosen route. An intermediary device attack is another name for this specific kind of cyberattack. According to the idea, an adversary who wishes to simulate a device first must determine a standard key with the equipment they want to imitate to succeed. Since it does not have the secret key that the TP provided, it cannot get the identical key that was computed by the device. It makes it impossible for it to do so. Because of this attack deciphering the PDLP and discovering the location of the secret key to TP might be challenging. Because of this, creating a fake electronic device that looks and functions just like the real thing is impossible.

This work is licensed under a Creative Commons Attribution 4.0 International License.

ACHIEVEMENT OF SIMULATION

The suggested routing system is put through rigorous testing using the Network Simulator(NS-2)[27], which includes running many simulations. Because Crypto system is a cryptography library with many tools for developing and maintaining a security protocol, we decided to incorporate it into our simulator. Crypto system also includes a wide range of encryption algorithms. The Two Ray Ground modeling is used to direct the movements of the network's sixty nodes as they span a 1,000×1,000-meter area. Table 1 presents a high-level description of the simulation's parameters in this section.

Table 1: Simulation Criteria

Restrictions	Rate
Initial energy	150J
MAC protocols	MAC/802.11
Mobility prototype	Double Ray base
packaging sizes	512 bytes
queuing size	250 packets
Routing protocols	The proposed protocol, SAODV
Simulation area	1000*1000
Simulation time	200 seconds
Traffic category	Constant Bit Rate (CBR)
Transmission energy	0.5 W

We evaluate the proposed protocol using three metrics and then compare it to the SAHODV protocol.

1) The "end-to-end delay" of a packet is the average time it requires to travel from its source to its destination.
2) A device's "overhead" is the mean number of messages received from all other devices during the route-setting phase.
3) Attackers compromised a total of this many devices throughout the period represented by the simulation.

The compromise of authentic devices poses a substantial threat that is difficult to defend. Defending against this danger is quite difficult. If a system has been hijacked, an attacker can monitor all communications and security procedures, as well as actually participate in route selection. It indicates that every piece of technology has a potential flaw. We develop several alternative black hole offensive attackers to test the durability of the proposed protocols when exposed to malicious nodes.

This work is licensed under a Creative Commons Attribution 4.0 International License.

Our goal is to determine how well the protocol can withstand these attacks. They try to join the selected route or pose as that of the destination, transmitting RREP packets when given an RREQ packet.

The end-to-end delay results are shown in Figure 1 [28] as a proportion of the total number of attackers. It is possible to show that the suggested protocol has a lower end-to-end potential value than the SAHODV protocol. It is since the tactic places emphasis on selecting the path that is both the safest and the shortest one. The suggested route is better than the SAHODV route since it is less probable that an intruder will be capable of infecting a device and join in the specified path. If an adversary joins the designated route, it can keep the packets they obtain for a more extended period. It provides them with additional time to examine the contents of the packets and extract the vital information within them. A package must travel for a lot longer to reach its destination.

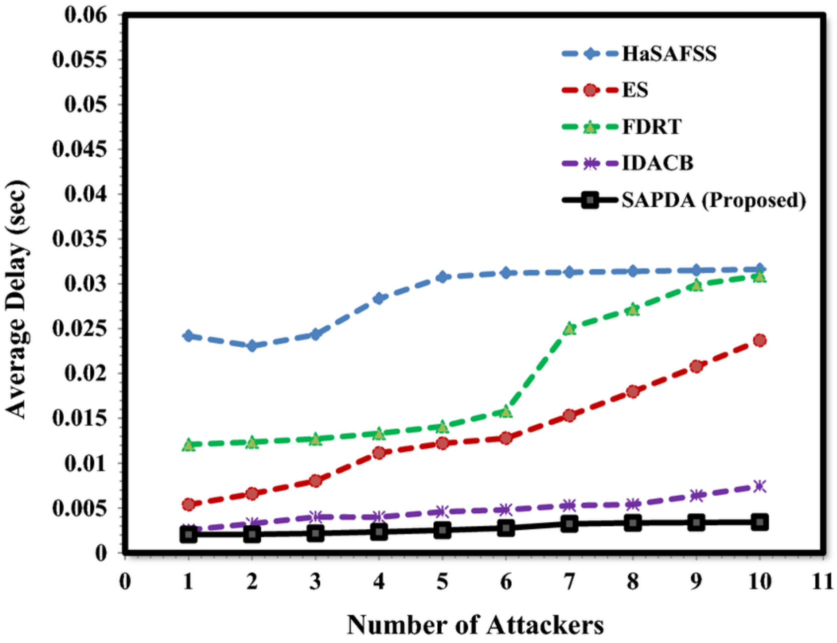

Figure 1: Delay vs Attacker Counts in End-to-end**[28]**

The findings of the overhead concerning the number of attackers are shown in Figure 2[29]. Compared to the SAHODV protocol, Because the number of attackers increases, the signal load necessary by the proposed protocol diminishes. The

This work is licensed under a Creative Commons Attribution 4.0 International License.

proposed systems that identify an attack packet will discard it, whereas, in SAHODV, devices will resend all packets they have received. In fact, according to our plan, the neighboring devices verify each other's identity by examining the encrypted packet's shared key. However, SAHODV fails to accomplish mutual authentication.

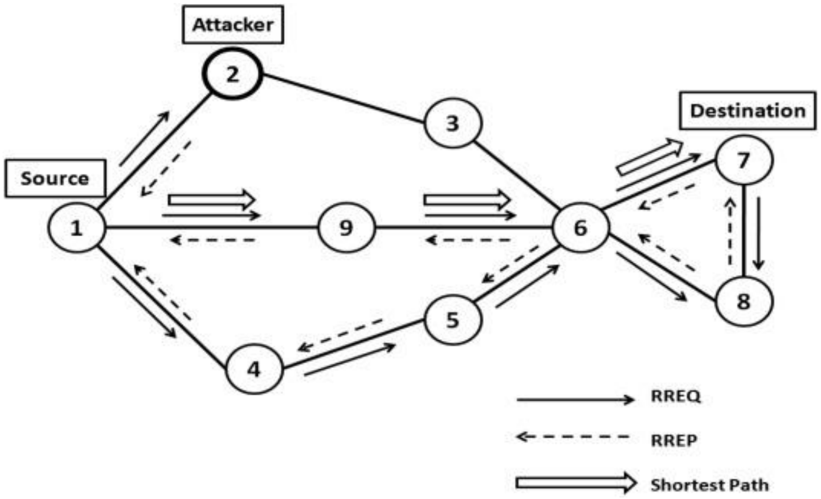

***Figure 2: Overhead vs Attackers Ratio*[29]**

Figure 3 indicates the consequences of the numbers of intruders lead as a representation of the numbers of infected machines. It is a description of the number of machines which have been infected. The method we have offered comprises many more devices than SAHODV, which means that it does not have the same effect. According to our methodology, the only key that is revealed when a device's security is breached is the device's private key. Because the adversary cannot generate digital certificates using these allowed devices, the integrity of these credentials has not been breached. The SAHODV protocol, on the other hand, only establishes mutual authentication between the source and the destination; hence it is conceivable for an adversary to compromise the victim's nearby devices and gain access to their data.

This work is licensed under a Creative Commons Attribution 4.0 International License.

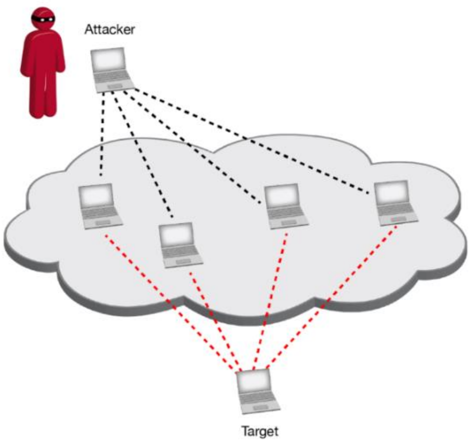

Figure 3: Number of Threats vs Number of infected Devices

CONCLUSION

The unique properties of MHWNs significantly impact data routing security between communicants. Indeed, various obstacles, such as the devices' limited battery life and storage space, must be overcome via a safe routing protocol in such a network. Because the routing also is handled step by step between normal nodes, it is simple for an adversary of this kind to cause damage to a portion of the network in addition to influencing the path that data will take in the end. Regarding this matter, we have suggested a method of routing for MHWN that is secure and effective. This strategy considers the minimum energy of the many devices along the route. In addition, a proposed method for binding agreement assures those security aspects such as authenticity and confidentiality are maintained throughout the routing process. Verifying the MAC operation also ensures its integrity. To ensure the safety of the request phase, we presumed that devices in proximity would use the Weil Pairing technique to generate shared keys among themselves. The parameters supplied during the request phase generate a shared secret key between the data's origin and destination to ensure its safety throughout transmission. To make the suggested protocol resilient against many attacks, we attempted to include low-cost cryptographic methods at each stage. To enhance the security of MHWNs, we want to implement an intrusion detection system in the future.

This work is licensed under a Creative Commons Attribution 4.0 International License.

ACKNOWLEDGEMENT

The researchers of this scientific paper are pleased to express their gratitude to everyone who helps us in the process of data collection for this study. My family and my friends are constantly available to lend their support to me in the endeavors I undertake.

REFERENCES

[1] V. U. Manfredi and C. Donnay Hill, “Quantifying unlinkability in multi-hop wireless networks,” *Comput. Commun.*, vol. 181, pp. 32–44, Jan. 2022, DOI: 10.1016/j.comcom.2021.09.022.

[2] V. Sabourin and J. T. Jabo, “Internet of Things,” in *IoT Benefits and Growth Opportunities for the Telecom Industry*, Boca Raton: CRC Press, 2022, pp. 7–12.

[3] K. Y. Abeywardena, A. M. I. S. Abeykoon, A. M. S. P. B. Atapattu, H. N. Jayawardhane, and C. N. Samarasekara, “ARCSECURE: Centralized Hub for Securing a Network of IoT Devices,” 2021, pp. 1071–1082.

[4] R. Alageswara, O. G. Kiruthiga, T. K. Keerthika, and B. Prakash, “Design and Development of Routing Protocol for WSN Simulation in GloMoSim,” *J. Artif. Intell.*, vol. 6, no. 2, pp. 181–186, Mar. 2013, doi: 10.3923/jai.2013.181.186.

[5] L. Naik. L, R. U.Khan, and R. B.Mishra, “MANETs: QoS and Investigations on Optimized Link State Routing Protocol,” *Int. J. Comput. Netw. Inf. Secure.*, vol. 10, no. 10, pp. 26–37, Oct. 2018, DOI: 10.5815/ijcnis.2018.10.04.

[6] K. M. Ali Alheeti, L. Al-Jobouri, D. Al-Dosary, and M. S. Al-ani, “Energy Conservation Based on Destination-Sequenced Distance-Vector Protocol in Intelligent Internet of Things,” in *2019 11th Computer Science and Electronic Engineering (CEEC)*, Sep. 2019, pp. 108–112, DOI: 10.1109/CEEC47804.2019.8974330.

[7] R. K. Singh and M. M. Chandane, “Dynamic Power Allocation in Wireless Routing Protocols,” 2016, pp. 91–97.

[8] M. A. Abdelshafy and P. J. B. King, “Dynamic source routing under attacks,” in *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, Oct. 2015, pp. 174–180, DOI: 10.1109/RNDM.2015.7325226.

[9] D. K. Kumaravel and D. M. Sengaliappan, “Performance Study on Multipath Routing Algorithm using Temporarily Ordered Routing Algorithm TORA using Link – Reversal in Wireless Networks,” *Int. J. Trend Sci. Res. Dev.*, vol. Volume-2, no. Issue-1, pp. 328–331, Dec. 2017, doi: 10.31142/ijtsrd5951.

[10] D. R. Madhanmohan, “A Study on Ad-Hoc on-Demand Distance Vector AODV Protocol,” *Int. J. Trend Sci. Res. Dev.*, vol. Volume-3, no. Issue-4, pp. 1019–1021, Jun. 2019, doi: 10.31142/ijtsrd24006.

[11] A. Said, “Devise Building and Routing protocols for the Internet of Things Mesh Networks,” MTI University, 2022.

[12] H. Zhang, “A WSN Clustering Multi-Hop Routing Protocol Using Cellular Virtual Grid in IoT Environment,” *Math. Probl. Eng.*, vol. 2020, pp. 1–7, Nov. 2020, DOI: 10.1155/2020/8886687.

[13] S. Glisic, “Multi-Hop Cellular Networks,” in *Advanced Wireless Networks*, Chichester, UK: John Wiley & Sons, Ltd, 2016, pp. 318–345.

[14] A. M. Jones, B. Rigling, and M. Rangaswamy, “Signal-to-interference-plus- noise-ratio analysis for constrained radar waveforms,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 5, pp. 2230–2241, Oct. 2016, doi: 10.1109/TAES.2016.150511.

[15] S. K. Biswash, A. Ziviani, R. Jain, J.-C. Lin, and J. J. P. C. Rodrigues, “Editorial: Device-to-Device Communication in 5G Networks,” *Mob. Networks Appl.*, vol. 22, no. 6, pp. 995–997, Dec. 2017, DOI: 10.1007/s11036-017-0828-7.

This work is licensed under a Creative Commons Attribution 4.0 International License.

[16] L.-L. Pan, “An optimization strategy for DSR protocol,” in *The 7th IEEE/International Conference on Advanced Infocomm Technology*, Nov. 2014, pp. 143–147, DOI: 10.1109/ICAIT.2014.7019545.

[17] S. S. et al., “Trust-based Routing Protocols in Wireless Networks,” *Turkish J. Comput. Math. Educ.*, vol. 12, no. 1S, pp. 567–572, Apr. 2021, doi: 10.17762/turcomat.v12i1S.1931.

[18] A. Vinitha, M. S. S. Rukmini, and Dhirajsunehra, “Secure and energy-aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 5, pp. 1857–1868, May 2022, doi: 10.1016/j.jksuci.2019.11.009.

[19] S. Jadhav, I. Panpaliya, and S. Jadhav, “Comparative Study of Low-Energy Adaptive Clustering Hierarchy Protocols,” 2022, pp. 325–339.

[20] Y.-M. Tseng, S.-S. Huang, and M.-L. “Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments,” *Int. J. Commun. Syst.*, vol. 30, no. 11, p. e3251, Jul. 2017, DOI: 10.1002/dac.3251.

[21] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, Jun. 2002, DOI: 10.1145/581291.581312.

[22] S. S. Wagstaff, “Private Key Ciphers,” in *Cryptanalysis of Number Theoretic Ciphers*, Chapman and Hall/CRC, 2019, pp. 221–230.

[23] S. O. Hwang, I. Kim, and W. K. Lee, “Hash Function,” in *Modern Cryptography with Proof Techniques and Applications*, CRC Press, 2021, pp. 87–102.

[24] S. Saha, U. Roy, and D. Sinha, “Application of RREQ Packet in Modified AODV(m-AODV) in the Contest of VANET,” 2015, pp. 489–502.

[25] B. K. Pattanayak, O. Pattnaik, and S. Pani, “Dealing with Sybil Attack in VANET,” 2021, pp. 471–480.

[26] M. Bartoletti *et al*., “Combining behavioural types with security analysis,” *J. Log. Algebr. Methods Program.*, vol. 84, no. 6, pp. 763–780, Nov. 2015, DOI: 10.1016/j.jlamp.2015.09.003.

[27] T. Issariyakul and E. Hossain, “Introduction to Network Simulator 2 (NS2),” in *Introduction to Network Simulator NS2*, Boston, MA: Springer US, 2012, pp. 21–40.

[28] N. Goyal, M. Dave, and A. K. Verma, “SAPDA: Secure Authentication with Protected Data Aggregation Scheme for Improving QoS in Scalable and Survivable UWSNs,” *Wirel. Pers. Commun.*, vol. 113, no. 1, pp. 1–15, Jul. 2020, doi: 10.1007/s11277-020-07175-8.

[29] M. Nosoohi, M. Ghasemzadeh, A. M. Z. Bidoki, and M. A. M. Abadi, “A trust-propagation-based scheme against pollution attacks in wireless network coding,” in *2011 International Symposium on Computer Networks and Distributed Systems (CNDS)*, Feb. 2011, pp. 131–135, DOI: 10.1109/CNDS.2011.5764559.

This work is licensed under a Creative Commons Attribution 4.0 International License.