Smart Internet of Things

www.siot.reapress.com

Smart. Internet. Things. Vol. 3, No. 3 (2026) 137–147.

Paper Type: Original Article

Secure Routing Protocols for Wireless Sensor Networks in IoT

Kushagra Srivastava*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22051945@kiit.ac.in.

Citation:

Received: 05 March 2026 *Revised: 28 May 2026* *Accepted: 12 August 2026*	Srivastava, K. (2026). Secure routing protocols for wireless sensor networks in IoT. *Smart Internet of Things, 3*(3), 137-147.

Abstract

The Internet of Things (IoT) has transformed global connectivity, supporting smart services and rapid response through edge computing, which improves both user experience and service resilience. Edge computing's proximity to users enhances quality of service, yet IoT networks remain vulnerable to security threats. Existing methods primarily rely on static sensor networks, limiting security against dynamic, mobile adversaries. To address this, we propose a secure routing and monitoring protocol utilizing a Two-Fish (TF) symmetric key mechanism within an Authentication and Encryption Model (ATE). By leveraging an Eligibility Weight Function (EWF), this protocol dynamically selects and conceals sensor guard nodes. Our hybrid approach integrates Multipath Optimized Link State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols, ensuring resilient, multipath data delivery. This approach demonstrates a higher percentage of active monitoring nodes and robust defense against mobile adversaries, securing IoT networks more effectively.

Keywords: IoT security, Edge computing, Multipath routing, Two-Fish encryption, Sensor guard nodes, Monitoring protocol.

1 | Introduction

The Internet of Things (IoT) is widely recognized as the driving force behind the "third industrial revolution," enabling devices to collect, share, and respond to physical data via the Internet. This revolution has grown at an impressive rate, from two billion connected objects in 2006 to an anticipated 200 billion by 2020, transforming fields such as education, finance, energy, healthcare, transportation, and urban planning into "smart" sectors. With these advancements, however, ensuring security within IoT networks has become essential to prevent data breaches and protect users. The rise of interconnected IoT applications, such as smart homes and vehicles, also increases the risk of cyber-attacks, highlighting the need for robust defenses.

A single vulnerability within an IoT system can compromise not just one component but potentially the entire network. For example, the 2016 Dyn cyberattack exploited IoT devices through malware (Mirai) to create

Corresponding Author: 22051945@kiit.ac.in

https://doi.org/10.48313/siot.v3i3.233

Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

large botnets, underscoring IoT systems' susceptibility to evolving cyber threats. Wireless Sensor Networks (WSNs), comprising nodes that gather and transmit data from various sensors (e.g., temperature, pressure), are particularly vulnerable because of their open wireless nature [1], [2].

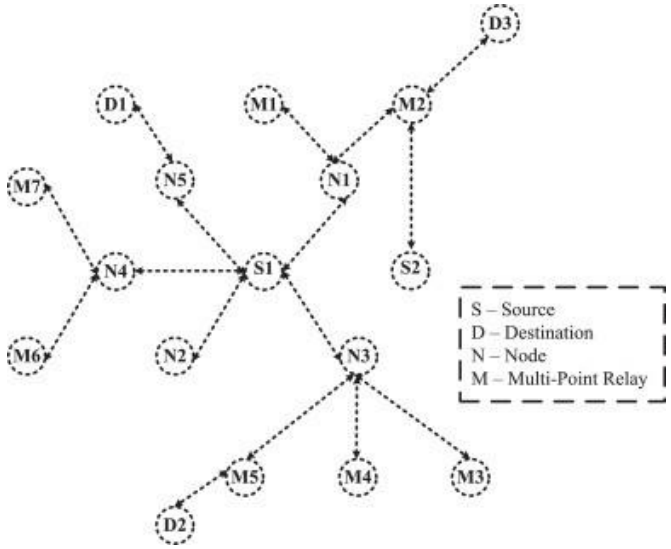

Fig.1. Initial network setup.

In defense and surveillance contexts, WSNs are valuable for detecting environmental changes and unauthorized activity, although securing these systems with minimal energy use is challenging. Mobile adversaries can target WSNs by intercepting data, modifying sensor behavior, or compromising node functionality, all of which impact network performance and reliability [3], [4].

To address these risks, Intrusion Detection Systems (IDS) are commonly employed to monitor and safeguard network integrity. While IDS technologies are traditionally used in wired networks, advancements in data mining, machine learning, and deep learning are paving the way for adaptive IoT security solutions. Researchers such as Agarwal et al. and Buczak et al. have investigated these approaches, while others, like Fadlullah and Hodo, explore deep learning's role in intrusion detection. This research aims to extend these methods for IoT, adapting IDS to dynamically detect and prevent security threats within complex IoT ecosystems [5–7].

Table 1. ImportantNotationUsed

Notation	Description
IoT	Internet of Things
VoA	Vulnerability of Attacks
TF	Two-Fish
ATE	Authentication and Encryption Model
EWF	Eligibility Weight Function
OLSR	Optimized Link State Routing (OLSR) and
AOMDV	Ad hoc On-Demand Multipath Distance Vector
DSDV	Destination Sequenced Distance Vector
TARCS	Topology Change Aware-Based Routing Protocol
WSN	Wireless Sensor Networks

Table 1. Continued.

Notation	Description
IDS	Intrusion Detection System
DIDS	Distributed Intrusion Detection System
BS	Base Station
CMS	Concealed Monitoring Set
QoS	Quality of Services
DSR	Dynamic Routing Protocol
MANET	Mobile Ad hoc Network
VCG	Vickrey, Clarke, and Groves
MPR	Multipoint Relays
ANSN	Advertised Neighbor Sequence Number
ANIA	Advertised Neighbor Information Address
INITREQ	Initial Request
INITRES	Initial Response
MaRES	Mask Request
MaREQ	Mask Response
HMAC	Hash-based Message Authentication Code
PSQN	Packet Sequence Number
MAC	Medium Access Control
RCP	Routing Control Packets
PIT	Protocol Interface Table
SRT	Sandwiched Routing Table
CBR	Constant Bit Rate
UDP	User Datagram Protocol
DCF	Distributed Coordination Function
KMP	Knuth–Morris–Pratt

2|Literature Review

In this section, we dive into the unique dance of algorithms designed to guide and safeguard routes within wireless sensor networks. Imagine the route identification Request (RREQ) as the opening move, setting the stage for secure data passage. Following this, the initial selection phase chooses the strongest, most reliable pathways, ensuring a smooth journey ahead [8–11].

Then, enter the secure monitors, chosen specifically to oversee multiple communication channels. Their role is akin to vigilant sentinels, stationed across the network to keep threats at bay. When needed, the algorithm initiates on-demand route maintenance, like a rapid response team, stepping in to fix and reroute data pathways in real time. With secure monitors at the helm, secure transmission becomes more than just a passage; it's a fortified journey, shielded against potential vulnerabilities. The monitors generate aggregated

reports, track each channel's status, and provide constant updates. Additionally, channel-dependent key shares further strengthen this communication, uniquely tailored to each channel to enhance confidentiality.

Together, these algorithms not only secure the communication within the network but also ensure that every bit of data travels safely and efficiently, demonstrating the intricate metrics at play in secure routing protocols.

Peer-to-Peer (P2P) systems have expanded rapidly due to their ability to distribute and share resources across large decentralized networks. A central challenge in these systems is the selection of high-capacity nodes to serve as super-peers, a process complicated by heterogeneous node capabilities and the dynamic nature of P2P environments. Recent studies highlight the need for capacity-aware protocols that can accurately identify the most suitable nodes for this role. Approaches based on SG-2 models and Gossip-based mechanisms—utilizing broadcast services, delay-distance metrics, and status exchanges among neighboring nodes—have demonstrated improved efficiency in selecting powerful super-peers. Such methods enhance overall network performance and reduce convergence time toward an optimal overlay structure, making them valuable for modern distributed architectures.

2.1 | Algorithms

Secure routing protocols in wireless sensor networks use several core algorithms for efficient, protected data transmission. Route Identification Request (RREQ) initiates path discovery and identifies secure routes. The Initial Selection Phase evaluates and chooses the optimal path. Secure Monitors oversee network traffic, detecting threats across multiple channels. The On-Demand Route Maintenance algorithm reroutes data when disruptions occur, ensuring continuous connectivity. Secure Transmission safeguards data with encryption and authentication, while Aggregated Monitor Report Generation provides regular updates on network health. Finally, Channel-Dependent Key Shares assign unique encryption keys per channel, adding a layer of security by isolating channels to prevent widespread compromise.

2.1.1 | Algorithm 1: Initial setup and neighbors identification using MPRs (SRC: ADDRESS; DST: ADDRESS; MSG: MESSAGE)

The algorithm in *Algorithm 1* kicks off with the initial steps of broadcasting a route request, brought to life in *Fig. 2*. Here, the journey begins with Source S sending out a friendly "hello" packet to scout the neighborhood. Its "hello" signals nearby nodes, seeking connections through Multipoint Relays (MPRs), guided by the proactive Optimized Link State Routing (OLSR) approach [12].

Before the MPRs fully form, the algorithm identifies unique link codes, mapping each link's mode and discovering neighboring nodes. These link codes act as a guide, laying out a network of potential pathways and allies in the neighborhood for future, secure communication.

Algorithm 1. Initial setup.

```
Hello Message: Initial setup
OLSR HELLO ()
{
        Step1: Source S broadcasts Hello Packets at time Tl;
        Step2: One hop Neighbors 'N1(s)' receive Hello Packets;
        Step3:  Ni of N1(s) checks Link Type of S; // Bidirectional
                    if (LC(0:1)&&LC(2:4)                    // Check Link Code LC
                        { Form MPR (s) of Ni;                  // Multipoint Relays
        Step4: MPR (s) retransmits Hello Packets to neighbors; // Two hop
        Step5: Do the same as Step 3 for N2i of N2(s); find seq. num;
        Step6: Find the path to destinations D;
        Step7: Redo (Periodically);
}}
```

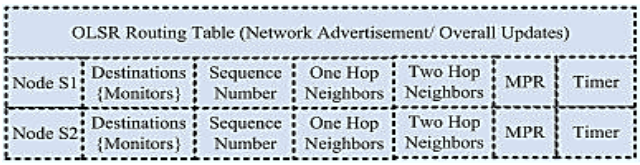

Fig. 2. OLSR routing table.

Algorithm 2 constructs one- and two-hop neighbor sets, minimizing redundant requests and responses. Additionally, the module below updates the OLSR link-state topology table by verifying the sequence of request and response counts. *Fig. 2* illustrates the OLSR routing table fields, presenting details for two source nodes and their respective destinations.

Algorithm 2. Neighbors identification using MPRs.

```
OLSR TC ()
{
Step1: Where Ti − >Ti + l; Ti - Current Time; l -Interval
        If (MPR(s)! = Null)
        {
        // Advertised Neighbor (Seq Number / InfAddr);
        Neighbors identify and check ANSN && ANIA;
        // Check Sequence Numbers
        If (ANSNi + l! < ANSNi)
        { Create TC Table};
        Else
        { Drop TC;}
        }
}
Step2: Redo at Ti +
```

2.1.2 | Algorithm 3: initial selection phase

The algorithm in *Algorithm 3* initiates the selection phase for neighbors that will serve as monitor nodes. Neighbors and paths are identified individually, reducing redundancy in routing communication. Source S sends an INITREQ (Initial Request) to neighbors located at one- and two-hop distances at random intervals, then waits for an INITRES (Initial Response) from these sensor nodes. This process accommodates multiple sources and destinations within the ad hoc sensor network, enhancing adaptability and reach across the network structure.

Algorithm 3. Initial selection.

```
OLSR INIT ()
 {
Step 1: If (N1i(s)!=Null&&N2i!==Null)
      {
Step 2: If (N1i||N2i not in MPR(s)) // Avoiding Redundancy
      {
      Set broadcast id=1;
      Send broadcast INITREQ message to qualified neighbors;
      Wait for Response;
      }
      Else
      Update Ni Table;
      }}
```

2.1.3|Algorithm 4: on demand route maintenance and secure transmission

After OLSR completes Connected Monitoring Set (CMS) formation, a timer triggers activation of AOMDV's on-demand monitoring strategy. At this point, AOMDV accesses node and neighbor details from OLSR through the Protocol Interface Table, a vital step in constructing the monitoring route path. AOMDV maintains this path in the AOMDV routing table, known as the Sandwich Routing Table, which layers both OLSR and AOMDV protocols. Algorithm 4 outlines this process, detailing on-demand monitoring and route maintenance across different channels to ensure robust, dynamic routing within the network.

Algorithm 4. On-demand route maintenance.

```
Step 1: If (Timer.OLSR = OFF)
{
AOMDV OP START()
{
addList.Ni ← (PI.T); addList.M, ←M(PI.T);
addList.DS ← DS(PI.T); addList.Ss ← Ss(PI.T);
Step 2: Mn generates RREQM; Get RESM;
Step 3: Mn builds route list (Multi-channels);
```

Algorithm 4. Continued.

```
`Build Concealed Monitor Sets (CMS);
Step 4: M executes PF (KMP) []
// Pattern Matching
If (EBit! = 1) // Check Link Error;;
{
If (PF! = PF1)
{ // Unsecure node or Channel (ID)
CID =  − 1 (error);
PI.T.RFlag = 1; Create PI.T.Report.M;
// MN-Malicious Node
[where PI.T.Report.M = =KMAC(Mln||CID||T)];
}
else
{S computes Cts = MACki||Rr{TFEki(MSGs)};
Here = 1….C, Rr-Maximum Rounds;
        At D, While (MAC = =MAC1)
        {Compute Pts = Rr{TFDki(Ct)};}
}
else
{Link error; (Mn (ERRM) → S through Next Hop);
}}
AODV OP WAIT/STOP
(updates PI.T.RFlag, PI.T.Report.M; Flush out AOMDV RTable)
}
Step 5: Set Timer.OLSR = ON; (after t seconds)}
```

2.1.4 | Algorithm 5: Aggregated monitor report generation

Algorithm 5 designates specific sensor nodes as monitors and equips them to run a pattern-matching function that scrutinizes node behavior and transmission traffic patterns, and verifies authenticity through HMAC (Hash-based Message Authentication Code). To secure data further, the Two fish encryption algorithm is applied, using channel-dependent key shares to tailor encryption to each communication channel. This layered approach ensures integrity and confidentiality, enabling monitor nodes to maintain secure, reliable data flows across the network [13], [14].

Algorithm 5. Monitoring report generation.

Step 1: (If Timer.OLSR = =ON)

{

Compute MPR(s); Update PI.T.Report.M in N(S);

N(s) search for route updates;

Continue transmission.

}

Step 2: Repeat the Algorithms.

3 | Results and Discussion

This section presents the simulation results for the proposed secure routing system, implemented using **Network Simulator Version 2.34 (NS-2.34) ** with OTCL (Object Tool Command Language). NS-2.34 was selected for its detailed capabilities in simulating mobile ad hoc networks, offering comprehensive insights into network topology, sensor nodes, network links, application protocols, and queuing mechanisms. The NS-2.34 simulation environment allowed for precise evaluation of the proposed routing protocol's performance and functionality.

The secure framework centered on three core components: detection, prediction, and isolation, with a focused analytical approach examining traffic generation patterns and routing mechanisms. Alternate NS versions proved inadequate for managing the required end-to-end connectivity and handling network load under various traffic conditions. Consequently, NS-2.34 was chosen to implement a secure hybrid routing protocol, which combines features from Multipath Optimized Link State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols. This hybrid protocol is designed to monitor sensor-node activity effectively, ensuring network security and stability [15].

Table 8 shows the simulation parameters. The MAC layer uses IEEE 802.11b, providing a transmission range of 140 meters. Node speeds vary between 0 m/s and 5 m/s, and their high mobility results in cluster formation. Testing included both existing and proposed routing protocols; however, neither performed optimally in highly dynamic environments. At the transport layer, the protocols utilize User Datagram Protocol (UDP), transmitting data at a constant bit rate (CBR) of 512 or 1024 bytes. Key communication metrics, including monitoring rate and detection ratio, were evaluated over a 500-second simulation period. Nodes were distributed within a 600 x 600-meter area, with malicious nodes randomly placed to study the impacts of mobility and data collision on network security.

Algorithm 6. Details of simulation parameters.

Constraints	Values
Network Size	600 m x 600 m
Number of Nodes	200 Nos.
Initial Energy	10 Joules
Simulation Time	100 S
Security Module	HMAC, TF-256 Bits, Key Generation
Routing Protocol	DSDV/OLSR/AOMDV/TARCS/Secure Hybrid Routing
Channel Model	Two-Ray Ground Propagation
Data Transmission Mode	Constant Bit Rate (CBR)
Antenna	Omni-Directional
Data Packet Size	512 / 1024 Bytes
Data Transmission Rate	16 Kbps
MAC Protocol	IEEE 802.11b, i.e., Distributed Coordination Function (DCF)
Range of Transmission	140m

4| Conclusion

The proposed hybrid routing and monitoring mechanism has been developed and implemented with dynamically selected sensor monitor nodes in ad hoc sensor networks to enhance secure data transmission. To ensure flexible security, a secure routing and monitoring protocol utilizing multi-variant tuples has been introduced, employing symmetric key algorithms such as MARS, RC6, Serpent, and Two-fish. This approach effectively identifies and mitigates adversarial threats within the global sensor network.

Built on the Authentication and Encryption Model (ATE), the mechanism incorporates an Eligibility Weight Function (EWF) to select sensor guard nodes using a complex symmetric-key approach. By leveraging the strengths of MARS, RC6, Serpent, and Two-fish, the hybrid system uses a node-selection algorithm that strengthens security through the strategic choice of sensor monitor nodes. This innovative design facilitates secure data transmission in the ad hoc sensor network while minimizing the impact of malicious activities.

Extensive simulations show that the proposed hybrid secure routing protocol achieves a higher monitoring rate and detection ratio than existing protocols.

Looking ahead, plans are in place to establish a real-time testbed to implement this hybrid routing and monitoring mechanism, enabling validation of the simulation results. Furthermore, this mechanism will be applied in IoT-based Wireless Sensor Networks (WSNs) to ensure the security and confidentiality of application environments, such as smart cities.

Author Contribution

I, K. S.: conceptualized the study, developed the methodology, wrote the initial draft, analyzed the data, implemented the necessary algorithms, and reviewed the final manuscript.

Funding

This research received no external funding.

Data Availability

The data used and analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Al-Turjman, F. (2020). Intelligence and security in big 5G-oriented IoNT: An overview. *Future Generation Computer Systems*, *102*, 357–368. https://doi.org/10.1016/j.future.2019.08.009

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, *38*(4), 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4

[3] Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials*, *10*(3), 6–28. https://doi.org/10.1109/COMST.2008.4625802

[4] Jokhio, S. H., Jokhio, I. A., & Kemp, A. H. (2012). Node capture attack detection and defence in wireless sensor networks. *IET Wireless Sensor Systems*, *2*(3), 161–169. https://doi.org/10.1049/iet-wss.2011.0064

[5] Abduvaliyev, A., Pathan, A.-S. K., Zhou, J., Roman, R., & Wong, W.-C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *15*(3), 1223–1237. https://doi.org/10.1109/SURV.2012.121912.00006

[6] Chen, R. C., Hsieh, C. F., & Huang, Y. F. (2010). An isolation intrusion detection system for hierarchical wireless sensor networks. *Journal of Networks*, *5*(3), 335–342. https://doi.org/10.4304/jnw.5.3.335-342

[7] Agrawal, S., & Agrawal, J. (2015). Survey on anomaly detection using data mining techniques. *Procedia Computer Science*, *60*, 708–713. https://doi.org/10.1016/j.procs.2015.08.220

[8] Mamun, M. S. I., & Kabir, A. F. M. S. (2010). Hierarchical design based intrusion detection system for wireless ad hoc sensor network. *International Journal of Network Security & Its Applications*, *2*(3), 102–117. https://doi.org/10.5121/ijnsa.2010.2307

[9] Yan, K. Q., Wang, S. C., & Liu, C. W. (2009). A hybrid intrusion detection system of cluster-based wireless sensor networks. In *Proceedings of the international multiconference of engineers and computer scientists* (Vol. 1, pp. 18-20). http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp411-416.pdf

[10] Lu, H., Li, J., & Wang, G. (2009). A novel energy efficient routing algorithm for hierarchically clustered wireless sensor networks. In *2009 Fourth International Conference on Frontier of Computer Science and Technology* (pp. 565-570). IEEE. https://doi.org/10.1109/FCST.2009.63

[11] Li, X., Mao, Y., & Liang, Y. (2008). A survey on topology control in wireless sensor networks. In *2008 10th International Conference on Control, Automation, Robotics and Vision* (pp. 251-255). IEEE. https://doi.org/10.1109/ICARCV.2008.4795527

[12] Toutouh, J., García-Nieto, J., & Alba, E. (2012). Intelligent OLSR routing protocol optimization for VANETs. *IEEE Transactions on Vehicular Technology*, *61*(4), 1884-1894. https://doi.org/10.1109/TVT.2012.2188552

[13] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. *IEEE Access*, *7*, 124379-124389. https://doi.org/10.1109/ACCESS.2019.2937347

[14] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25-37. https://doi.org/10.1016/j.jnca.2017.02.009

[15] Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE Communications Surveys & Tutorials*, *20*(4), 3496–3509. https://doi.org/10.1109/COMST.2018.2844742