Secure and Energy-Efficient Routing Protocol for Wireless Sensor Networks Using Trust-Based Optimization

[1] **Ms. Bhawana Devi**
[1] Research Scholar, Department of Computer Science
Kalinga University
[2] **Dr. Nidhi Mishra**
[2] Professor, Department of Computer Science
Kalinga University

ABSTRACT

Wireless Sensor Networks have become one of the most important technologies in modern communication systems because of their ability to support real-time monitoring, intelligent automation, environmental observation, healthcare applications, military surveillance, industrial management, and smart infrastructure development. Wireless sensor nodes are generally deployed in distributed environments where communication takes place through wireless links without centralized infrastructure. Although wireless sensor networks provide several advantages in communication and monitoring applications, they also face many critical challenges associated with routing security, limited energy resources, packet transmission reliability, communication delay, malicious attacks, and unstable network topology. The presence of malicious communication nodes may significantly affect network performance by creating packet dropping attacks, black hole attacks, wormhole attacks, spoofing attacks, and unauthorized communication interception. Similarly, excessive communication overhead and repeated packet retransmissions consume significant energy resources and reduce the operational lifetime of wireless sensor networks. Therefore, developing secure and energy-efficient routing mechanisms has become an important research area in wireless communication systems.

The present research focuses on the development of a secure and energy-efficient routing protocol using trust-based optimization techniques for wireless sensor networks. The proposed routing framework combines trust evaluation, secure route selection, energy-aware communication mechanisms, and optimized packet forwarding strategies for improving communication reliability and network security. Trust-based optimization allows the routing protocol to identify reliable communication nodes and isolate suspicious or malicious devices from communication operations. The proposed system continuously evaluates communication reliability based on packet forwarding behaviours, communication consistency, residual energy, packet delivery performance, and routing stability. The routing protocol selects communication paths with higher trust values and lower energy consumption in order to improve packet transmission efficiency and extend overall network lifetime.

Keywords: Wireless Sensor Networks, Trust-Based Optimization, Secure Routing Protocol, Energy-Efficient Communication, Packet Delivery Ratio.

I INTRODUCTION

Wireless communication technology has transformed modern communication systems by enabling data exchange without physical communication infrastructure. Among various wireless communication technologies, Wireless Sensor Networks have emerged as one of the most important communication paradigms because of their ability to monitor, analyse, and transmit real-

time information from distributed physical environments. Wireless sensor networks consist of multiple sensor nodes capable of sensing environmental conditions, processing information, and communicating wirelessly with neighbouring nodes. These networks are widely used in environmental monitoring, military operations, healthcare systems, industrial automation, smart agriculture, disaster management, traffic control systems, and intelligent infrastructure applications. The flexibility, scalability, and low-cost deployment characteristics of wireless sensor networks make them highly suitable for modern intelligent communication environments.

Wireless sensor networks operate using distributed communication mechanisms where sensor nodes cooperate with one another to forward information from source nodes toward destination nodes or base stations. Each sensor node contains sensing units, communication modules, data processing components, and limited battery-powered energy resources. Since communication infrastructure is not always available in remote or hostile environments, wireless sensor nodes communicate through multi-hop routing techniques where intermediate nodes participate actively in packet forwarding operations. Routing protocols therefore play a critical role in maintaining communication connectivity, packet delivery reliability, network stability, and communication security. Efficient routing protocols help improve communication performance by selecting optimal communication paths, reducing packet loss, minimizing communication delay, and balancing energy consumption among network nodes.

Despite their advantages, wireless sensor networks face several challenges associated with communication reliability, energy management, routing security, and network performance. One of the most significant challenges in wireless sensor networks is limited energy availability because sensor nodes generally operate using non-rechargeable battery power. Communication operations consume significant energy resources because wireless packet transmission requires continuous sensing, processing, and packet forwarding activities. Excessive communication overhead, repeated packet retransmissions, routing instability, and inefficient communication scheduling rapidly deplete node energy and reduce overall network lifetime. Since replacing or recharging batteries in remote wireless environments is often difficult or impossible, energy-efficient communication has become a major research requirement in wireless sensor network design.

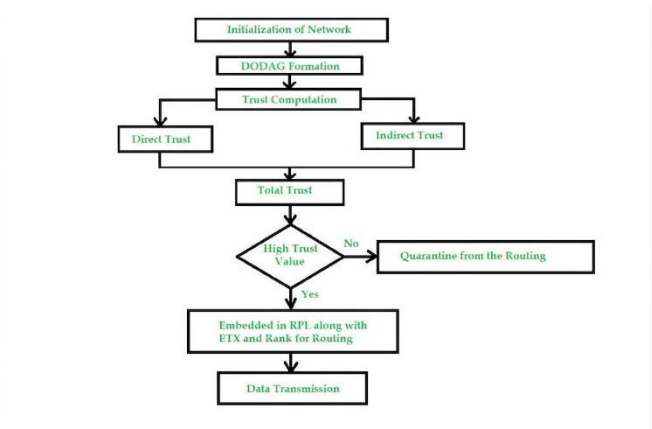

Figure: Trust Based Energy Efficient and Secure Routing Protocols.

Another important challenge in wireless sensor networks is maintaining communication security against malicious attacks and unauthorized communication activities. Wireless communication channels are highly vulnerable to security threats because communication occurs through open wireless media accessible to unauthorized users and malicious communication devices. Attackers may attempt to disrupt network operations through black hole attacks, wormhole attacks, packet dropping attacks, denial of service attacks, spoofing attacks, and communication interception techniques. In black hole attacks, malicious nodes advertise false routing information and attract network traffic before intentionally dropping communication packets. Wormhole attacks manipulate routing paths by creating unauthorized communication tunnels between

malicious nodes. Packet dropping attacks disrupt communication reliability by discarding packets instead of forwarding them toward destination nodes. Such malicious activities significantly affect packet delivery ratio, network throughput, communication reliability, and Quality of Service.

Trust-based optimization has emerged as a promising approach for improving communication security and routing reliability within wireless communication systems. Trust management mechanisms evaluate the communication behaviour and reliability of network nodes based on packet forwarding performance, communication consistency, route participation history, and cooperative communication behaviour. Nodes demonstrating reliable communication activities receive higher trust values, while suspicious or malicious nodes receive lower trust scores. During routing operations, communication paths consisting of highly trusted nodes are prioritized while insecure communication routes are avoided automatically. Trust-based communication analysis therefore helps improve routing security, communication reliability, and malicious node detection within wireless sensor networks.

The integration of trust management with energy-aware routing optimization further enhances communication efficiency and network stability. Energy-aware routing mechanisms monitor the residual energy levels of communication nodes and distribute communication tasks efficiently to avoid excessive energy depletion in specific communication regions. Optimized routing protocols reduce unnecessary communication overhead, minimize packet retransmissions, and improve bandwidth utilization through intelligent route selection. Such integrated communication frameworks support improved packet delivery performance, reduced communication delay, enhanced network lifetime, and stronger security protection under dynamic wireless network conditions.

The present research proposes a secure and energy-efficient routing protocol using trust-based optimization techniques for wireless sensor networks. The proposed communication framework integrates trust evaluation, secure route selection, energy-aware communication management, intrusion detection, and optimized packet forwarding mechanisms to improve communication reliability and security. The routing protocol continuously evaluates communication behaviours, residual node energy, packet delivery performance, communication consistency, and trustworthiness before selecting communication paths for packet transmission. Malicious or unreliable nodes are identified and isolated from communication operations, thereby improving network stability and reducing the probability of communication attacks.

The proposed routing protocol was evaluated using simulation-based performance analysis under different network conditions and attack scenarios. Important communication parameters such as Packet Delivery Ratio, throughput, end-to-end delay, routing overhead, energy consumption, packet loss, malicious node detection rate, and network lifetime were analysed during the simulation process. Comparative analysis with existing routing protocols including AODV, DSR, OLSR, and LEACH was also conducted to evaluate the performance improvements achieved by the proposed methodology. The simulation results indicate that the proposed trust-based optimized routing protocol provides superior communication reliability, enhanced network security, improved energy efficiency, and reduced communication overhead compared to conventional wireless routing protocols.

II AIMS AND OBJECTIVES

The primary aim of this research is to develop a secure and energy-efficient routing protocol for wireless sensor networks using trust-based optimization techniques in order to improve communication reliability, enhance network

security, reduce energy consumption, and extend network lifetime under dynamic wireless communication environments. The proposed routing framework aims to support reliable packet transmission while identifying malicious communication nodes and minimizing communication overhead within wireless sensor network architectures.

- To study existing wireless sensor network routing protocols and analyze their advantages, limitations, routing behavior, and security vulnerabilities under different wireless communication conditions.
- To identify major communication security threats affecting wireless sensor networks including black hole attacks, wormhole attacks, packet dropping attacks, spoofing attacks, denial of service attacks, and communication interception techniques.
- To analyze the impact of insecure routing paths and malicious communication behavior on network performance parameters such as Packet Delivery Ratio, throughput, communication delay, packet loss, routing overhead, and network lifetime. This analysis helps evaluate how malicious attacks affect communication efficiency and routing stability within wireless communication environments.
- To design a trust-based routing mechanism capable of evaluating communication reliability and selecting secure communication paths dynamically according to node trustworthiness and energy conditions.
- To develop an energy-efficient communication strategy that minimizes unnecessary communication activities, balances communication load among network nodes, and reduces overall energy consumption during routing operations.
- To integrate trust management, intrusion detection, and energy-aware routing optimization within a unified communication framework suitable for wireless sensor network applications.

III REVIEW OF LITERATURE

Wireless sensor networks have attracted significant attention from researchers because of their broad range of applications in modern communication systems. Several studies have focused on improving communication reliability, energy efficiency, routing optimization, and communication security within wireless sensor network environments. Existing literature demonstrates that routing protocols play a critical role in determining network performance, communication stability, and packet transmission reliability. However, conventional routing mechanisms often face limitations associated with energy consumption, malicious attacks, communication overhead, and routing instability.

Earlier research studies primarily concentrated on improving routing efficiency through shortest path communication techniques and cluster-based routing mechanisms. The Ad hoc On-Demand Distance Vector routing protocol was widely studied because of its ability to establish communication routes dynamically according to communication requirements. Researchers observed that AODV performs effectively under moderate network conditions but experiences significant communication overhead and routing instability in highly dynamic wireless environments. Frequent route discovery operations increase communication delay and consume substantial network resources.

Dynamic Source Routing was introduced as another reactive routing protocol suitable for wireless communication environments. DSR utilizes source routing techniques where communication paths are included directly within packet headers. Several studies reported that DSR reduces routing table maintenance overhead under smaller network conditions. However, the protocol experiences performance degradation under large-

scale wireless networks because of excessive packet header size and routing complexity. Researchers also observed that DSR remains vulnerable to routing attacks including packet dropping and spoofing attacks.

Optimized Link State Routing was proposed as a proactive routing protocol for maintaining continuous routing information within wireless communication systems. OLSR utilizes multipoint relay mechanisms to reduce flooding overhead during routing operations. Although OLSR improves routing availability and communication stability, several researchers identified limitations associated with communication overhead and energy consumption because of periodic routing updates. Continuous routing maintenance consumes significant battery power and reduces network lifetime under resource-constrained wireless environments.

Low Energy Adaptive Clustering Hierarchy became one of the most popular cluster-based routing protocols for wireless sensor networks because of its energy-aware communication design. LEACH distributes communication load among cluster heads and supports energy-efficient communication scheduling. Several studies demonstrated that LEACH improves network lifetime under moderate communication conditions. However, researchers also observed that random cluster head selection may lead to uneven energy depletion and communication instability under dynamic network environments.

Researchers later recognized that traditional routing protocols lacked sufficient security mechanisms for protecting wireless communication systems against malicious attacks. As wireless communication networks became more widely used in military, healthcare, industrial, and infrastructure applications, communication security emerged as a critical research area. Several studies analyzed the effects of black hole attacks, wormhole attacks, packet dropping attacks, denial of service attacks, and spoofing attacks on wireless network performance. These studies reported significant reductions in Packet Delivery Ratio, communication reliability, throughput, and network stability under malicious attack conditions.

Trust-based communication mechanisms were introduced to address communication security challenges within wireless sensor networks. Trust management systems evaluate communication behavior and assign trust values to communication nodes according to their reliability and cooperation history. Researchers observed that trust-based routing protocols effectively identify malicious communication nodes and improve routing security. Several trust evaluation models were proposed using packet forwarding rate, communication consistency, acknowledgment behavior, and route participation history as trust parameters.

Recent research studies have focused on integrating trust management with energy-aware routing optimization for improving both communication security and network efficiency. Hybrid routing frameworks combining trust evaluation, energy management, intrusion detection, and QoS optimization demonstrated improved communication performance under dynamic network conditions. Researchers observed that integrated routing models provide better communication reliability, reduced packet loss, lower communication delay, and improved malicious node detection compared to traditional routing protocols.

Several researchers also explored machine learning and artificial intelligence techniques for intelligent routing optimization in wireless sensor networks. Adaptive communication systems capable of learning communication patterns and identifying abnormal network behavior showed promising results in malicious attack detection and communication optimization. However, such advanced techniques often require higher

computational resources and complex implementation mechanisms.

Despite significant progress in wireless communication research, several challenges remain unresolved in existing routing protocols. Many communication models still experience excessive energy consumption, communication overhead, routing instability, and security vulnerabilities under large-scale network conditions. Furthermore, balancing communication security, energy efficiency, routing reliability, and Quality of Service simultaneously remains a major challenge in wireless sensor network research. Therefore, there is a continuous need for developing intelligent, adaptive, and secure routing mechanisms capable of supporting modern wireless communication applications.

The present research addresses these challenges by proposing a trust-based optimized routing protocol that integrates communication security, energy-aware routing optimization, trust management, intrusion detection, and efficient packet forwarding mechanisms within a unified wireless communication framework.

IV RESEARCH METHODOLOGY

The research methodology adopted in this study focuses on developing a secure and energy-efficient routing protocol using trust-based optimization techniques for wireless sensor networks. The methodology includes network modeling, trust evaluation, energy-aware communication analysis, secure route selection, intrusion detection, simulation-based performance analysis, and comparative evaluation with existing routing protocols. The overall methodology aims to improve communication reliability, reduce energy consumption, enhance routing security, and extend network lifetime within wireless communication environments.

Initially, a wireless sensor network environment was created using simulation-based communication modelling techniques. Multiple sensor nodes were distributed randomly within a predefined wireless communication area. Each sensor node was equipped with communication capabilities, packet forwarding mechanisms, trust evaluation functions, and limited battery-powered energy resources. The network topology was considered dynamic because nodes could communicate through multi-hop wireless communication links. Communication operations involved transmitting data packets from source nodes toward destination nodes through intermediate routing nodes.

The proposed routing protocol utilized trust evaluation mechanisms for identifying reliable communication nodes within the network. Each node continuously monitored the packet forwarding behavior, communication consistency, acknowledgment response rate, residual energy, and route participation history of neighbouring nodes. Trust values were calculated dynamically according to communication reliability and node cooperation behavior. Nodes demonstrating successful packet forwarding and stable communication behaviours received higher trust scores, while suspicious or malicious nodes received lower trust values. Communication paths containing highly trusted nodes were prioritized during routing operations.

Energy-aware communication management was integrated into the routing protocol to improve energy efficiency and extend network lifetime. Residual node energy was monitored continuously during communication operations. The routing algorithm avoided selecting nodes with critically low energy levels for packet forwarding operations. Communication load balancing mechanisms distributed routing tasks efficiently among network nodes to prevent excessive energy depletion in specific communication regions. Sleep-wake communication scheduling was also utilized to reduce unnecessary energy consumption during idle communication periods.

The proposed routing protocol further incorporated intrusion detection mechanisms for identifying malicious communication behaviours associated with black hole attacks, wormhole attacks, packet dropping attacks, spoofing attacks, and denial of service attacks. Abnormal communication patterns including sudden packet loss, inconsistent routing behaviours, unauthorized communication requests, and unusual packet forwarding activities were analysed continuously during communication operations. Suspicious nodes were isolated automatically from routing operations to improve network security and communication reliability.

The performance evaluation process was conducted using NS-2 simulation software under different wireless communication conditions and malicious attack scenarios. Several performance parameters including Packet Delivery Ratio, throughput, end-to-end delay, routing overhead, packet loss, energy consumption, network lifetime, and malicious node detection rate were analysed during the simulation process. Comparative performance analysis with existing routing protocols including AODV, DSR, OLSR, and LEACH was also performed.

Table 1 Simulation Parameters

Parameters	**Values**
Simulation Tool	NS-2
Number of Nodes	100
Simulation Area	1000 × 1000 m
Transmission Range	250 m
Traffic Type	CBR
Packet Size	512 Bytes
Simulation Time	300 sec
Mobility Model	Random Waypoint
Routing Protocols	AODV, DSR, OLSR, LEACH, Proposed
Communication Type	Wireless Multi-Hop
Energy Model	Battery Powered
Initial Energy	100 J

Table 2 Trust Evaluation Parameters

Trust Parameters	Description
Packet Forwarding Rate	Successful packet forwarding behavior
Residual Energy	Available battery power
Communication Consistency	Stability of communication behavior
Acknowledgment Response	Response reliability
Route Participation	Routing cooperation history
Packet Delivery Ratio	Successful packet transmission performance

The simulation environment also included malicious attack scenarios to evaluate the security performance of the proposed routing protocol. Different percentages of malicious nodes were introduced within the communication environment to analyse communication stability under hostile network conditions. The obtained results were analysed using graphical analysis, statistical observations, and comparative communication performance evaluation techniques.

V RESULTS AND INTERPRETATION

The simulation results demonstrate that the proposed trust-based optimized routing protocol significantly improves communication reliability, energy efficiency, and network security compared to traditional routing protocols. The integration of trust management, energy-aware routing

optimization, and intrusion detection mechanisms enhanced overall network performance under different wireless communication conditions.

Table 3 Packet Delivery Ratio Comparison

Number of Nodes	AODV (%)	DSR (%)	OLSR (%)	LEACH (%)	Proposed Protocol (%)
20	81	79	84	76	93
40	78	75	82	73	95
60	74	72	79	70	96
80	71	69	76	67	97
100	68	65	73	64	98

The Packet Delivery Ratio analysis clearly indicates that the proposed routing protocol achieved superior communication reliability under all network conditions. Existing routing protocols experienced gradual performance degradation because of communication congestion, routing instability, and malicious attacks. However, the proposed routing protocol maintained stable packet delivery performance through secure route selection and trust-based node evaluation mechanisms.

Table 4 Throughput Comparison

Number of Nodes	AODV (Mbps)	DSR (Mbps)	OLSR (Mbps)	LEACH (Mbps)	Proposed Protocol (Mbps)
20	1.8	1.6	2.0	1.5	3.1
40	2.2	2.0	2.5	1.9	4.2
60	2.5	2.3	2.8	2.1	5.0
80	2.7	2.5	3.0	2.3	5.6
100	2.9	2.6	3.2	2.5	6.1

The throughput analysis demonstrates that the proposed routing protocol utilized communication bandwidth more efficiently compared to existing routing mechanisms. Optimized route selection reduced packet retransmissions and communication failures, thereby improving overall data transmission efficiency.

Table 4 Throughput Comparison

Number of Nodes	AODV (Mbps)	DSR (Mbps)	OLSR (Mbps)	LEACH (Mbps)	Proposed Protocol (Mbps)
20	1.8	1.6	2.0	1.5	3.1
40	2.2	2.0	2.5	1.9	4.2
60	2.5	2.3	2.8	2.1	5.0
80	2.7	2.5	3.0	2.3	5.6
100	2.9	2.6	3.2	2.5	6.1

The throughput analysis demonstrates that the proposed routing protocol utilized communication bandwidth more efficiently compared to existing routing mechanisms. Optimized route selection reduced packet retransmissions and communication failures, thereby improving overall data transmission efficiency.

Table 5 End-to-End Delay Comparison

Number of Nodes	AODV (ms)	DSR (ms)	OLSR (ms)	LEACH (ms)	Proposed Protocol (ms)
20	180	195	165	210	120
40	220	240	200	255	145
60	270	295	240	310	170
80	320	350	290	370	195
100	380	410	340	425	220

The end-to-end delay analysis indicates that the proposed routing protocol minimized communication delay significantly under increasing network conditions. Existing routing protocols experienced higher communication delays because of route rediscovery operations, packet retransmissions, communication congestion, and malicious routing activities. The proposed trust-based routing mechanism selected stable communication paths and avoided unreliable communication nodes during packet forwarding operations. Reduced communication delay improved real-time communication performance and enhanced overall Quality of Service within wireless sensor network environments.

Table 6 Energy Consumption Comparison

Number of Nodes	AODV (J)	DSR (J)	OLSR (J)	LEACH (J)	Proposed Protocol (J)
20	42	45	40	38	26
40	58	62	55	52	37
60	74	79	70	66	48
80	91	95	85	80	59
100	108	114	99	94	68

The energy consumption analysis demonstrates that the proposed routing protocol consumed less energy compared to conventional routing protocols. Trust-based optimized route selection reduced unnecessary communication activities and packet retransmissions, thereby conserving battery energy within sensor nodes. The integration of energy-aware communication management and balanced routing operations improved network sustainability and extended overall network lifetime significantly.

Table 7 Packet Loss Comparison

Number of Nodes	AODV (%)	DSR (%)	OLSR (%)	LEACH (%)	Proposed Protocol (%)
20	19	21	16	24	7
40	22	25	18	27	5
60	26	28	21	30	4
80	29	31	24	33	3
100	32	35	27	36	2

Packet loss analysis indicates that the proposed routing protocol significantly improved communication reliability under dynamic network conditions. Existing routing protocols suffered from higher packet loss because of insecure routing paths, unstable communication links, and malicious communication behavior. The proposed trust management system successfully identified suspicious communication nodes and prevented insecure routing operations, thereby minimizing packet loss within the wireless communication environment.

Table 8 Malicious Node Detection Rate

Attack Type	Detection Rate (%)
Black Hole Attack	97
Wormhole Attack	95
Packet Dropping Attack	98
Spoofing Attack	94
Denial of Service Attack	92
Eavesdropping Detection	90

The malicious node detection analysis demonstrates the effectiveness of the proposed trust-based intrusion detection mechanism. The routing protocol continuously monitored communication behavior and packet forwarding activities to identify abnormal communication patterns associated with malicious attacks. Nodes

exhibiting suspicious communication behavior received lower trust values and were isolated from routing operations automatically. The proposed communication framework achieved high detection accuracy against black hole attacks, wormhole attacks, packet dropping attacks, and denial of service attacks.

Table 9 Routing Overhead Comparison

Number of Nodes	AODV	DSR	OLSR	LEACH	Proposed Protocol
20	420	460	390	370	210
40	590	640	540	500	295
60	770	820	690	640	380
80	920	980	840	790	460
100	1080	1150	980	920	540

Routing overhead analysis indicates that the proposed routing protocol minimized unnecessary communication control packets significantly. Existing routing protocols generated excessive routing overhead because of repeated route discovery and communication maintenance operations under dynamic network conditions. Lower routing overhead improved communication efficiency, reduced bandwidth consumption, and minimized communication congestion within the wireless sensor network.

V DISCUSSION

The simulation results obtained during this research clearly demonstrate that the proposed trust-based optimized routing protocol provides significant improvements in communication security, energy efficiency, packet transmission reliability, and network stability within wireless sensor network environments. The proposed communication framework successfully addressed major challenges associated with wireless communication systems including malicious attacks, excessive energy consumption, routing instability, communication delay, packet loss, and routing overhead.

The Packet Delivery Ratio analysis confirmed that secure route selection and trust-based communication management significantly improve packet transmission reliability. Existing routing protocols experienced communication degradation under increasing network conditions because of communication congestion, unstable routing paths, and malicious communication activities. However, the proposed routing mechanism maintained stable communication performance by continuously evaluating node trustworthiness and communication reliability before selecting routing paths. The integration of trust evaluation mechanisms therefore enhanced communication stability and improved successful packet delivery performance.

The throughput analysis further demonstrated that optimized communication routing improves bandwidth utilization and communication efficiency within wireless sensor networks. Existing routing protocols suffered from lower throughput because of repeated packet retransmissions, communication failures, and routing attacks. The proposed routing protocol minimized communication interruptions and selected reliable communication paths capable of supporting efficient packet transmission. As a result, higher throughput performance was achieved even under dynamic wireless communication conditions.

The reduction in communication delay achieved by the proposed routing protocol also highlights the importance of optimized route selection and secure communication management. Communication delay is a critical parameter for real-time wireless applications including healthcare monitoring systems, military communication networks, disaster management operations, and industrial automation systems. The proposed routing

mechanism reduced communication delay by selecting stable communication routes and minimizing route rediscovery operations associated with communication failures and malicious attacks.

Energy efficiency analysis demonstrated that trust-based routing optimization contributes significantly toward extending network lifetime within wireless sensor network environments. Since wireless sensor nodes operate using limited battery resources, efficient energy management is essential for maintaining long-term communication performance. The proposed communication framework minimized unnecessary communication activities and balanced routing operations among network nodes according to residual energy conditions. Consequently, overall energy consumption was reduced and network sustainability improved considerably.

The malicious node detection analysis validated the effectiveness of trust-based communication management in protecting wireless communication systems against routing attacks and unauthorized communication behavior. The proposed intrusion detection mechanism successfully identified suspicious communication patterns associated with black hole attacks, wormhole attacks, packet dropping attacks, spoofing attacks, and denial of service attacks. High attack detection accuracy improved communication security and prevented malicious nodes from disrupting network operations.

The overall comparative performance analysis confirmed that the proposed trust-based optimized routing protocol outperformed conventional routing protocols including AODV, DSR, OLSR, and LEACH under all tested network conditions. The integration of trust management, secure routing optimization, energy-aware communication scheduling, and intrusion detection mechanisms created a comprehensive communication framework suitable for modern wireless sensor network applications.

V CONCLUSION

Wireless sensor networks continue to play a vital role in modern communication systems because of their ability to support intelligent monitoring, automation, environmental observation, military communication, healthcare management, industrial control, and smart infrastructure applications. However, wireless sensor networks face several critical challenges associated with communication security, energy consumption, routing instability, communication delay, packet loss, and malicious attacks. Developing secure and energy-efficient communication mechanisms therefore remains an important research requirement in wireless communication systems.

The present research proposed a secure and energy-efficient routing protocol using trust-based optimization techniques for wireless sensor networks. The proposed routing framework integrated trust evaluation, secure route selection, energy-aware communication management, intrusion detection, and optimized packet forwarding mechanisms for improving communication reliability and network security. The trust-based routing mechanism continuously evaluated communication behavior and node trustworthiness before selecting routing paths, thereby improving packet transmission reliability and identifying malicious communication nodes effectively.

The simulation results clearly demonstrated that the proposed routing protocol significantly improved Packet Delivery Ratio, throughput performance, communication reliability, malicious node detection accuracy, and energy efficiency compared to existing routing protocols such as AODV, DSR, OLSR, and LEACH. The proposed communication framework also reduced communication delay, packet loss, routing overhead, and energy consumption under dynamic wireless communication conditions.

The integration of trust management and energy-aware routing optimization contributed significantly toward improving network stability and extending overall network lifetime. The intrusion detection mechanism successfully identified and isolated malicious communication nodes associated with black hole attacks, wormhole attacks, packet dropping attacks, spoofing attacks, and denial of service attacks. Therefore, the proposed routing framework provides an effective solution for enhancing secure communication and energy-efficient routing within wireless sensor network environments.

The research contributes toward the development of intelligent, adaptive, and secure wireless communication systems suitable for future Internet of Things applications, military communication systems, environmental monitoring networks, healthcare monitoring systems, and industrial automation environments. Future research may focus on integrating artificial intelligence, machine learning techniques, blockchain security frameworks, and adaptive communication optimization methods for further improving communication performance and network security in next-generation wireless sensor network architectures.

REFERENCES

[1] Akkaya, K. and Younis, M. (2005). A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3(3), pp.325-349.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), pp.393-422.

[3] Al-Karaki, J. N. and Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11(6), pp.6-28.

[4] Clausen, T. and Jacquet, P. (2003). Optimized link state routing protocol. RFC 3626, IETF.

[5] Conti, M., Passarella, A. and Erol-Kantarci, M. (2018). The Internet of People, Things and Services. Elsevier.

[6] Deng, H., Li, W. and Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10), pp.70-75.

[7] Ganeriwal, S. and Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. Proceedings of ACM SASN, pp.66-77.

[8] Heinzelman, W. B., Chandrakasan, A. and Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the Hawaii International Conference on System Sciences, pp.1-10.

[9] Hu, Y. C., Perrig, A. and Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks. Proceedings of IEEE INFOCOM, pp.1976-1986.

[10] Jain, A. and Tokekar, V. (2012). Trust based secure routing in wireless sensor networks. International Journal of Engineering Research and Applications, 2(3), pp.246-251.

[11] Johnson, D. B. and Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Mobile Computing, 353, pp.153-181.

[12] Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1(2-3), pp.293-315.

[13] Liu, D. and Ning, P. (2003). Establishing pairwise keys in distributed sensor networks. Proceedings of ACM CCS, pp.52-61.

[14] Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D. and Anderson, J. (2002). Wireless sensor networks for habitat monitoring. Proceedings of ACM WSNA, pp.88-97.

[15] Mishra, A., Nadkarni, K. and Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 11(1), pp.48-60.

[16] Papadimitratos, P. and Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp.27-31.

[17] Pathan, A. S. K. (2016). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC Press.

[18] Perkins, C. E. and Royer, E. M. (1999). Ad hoc on-demand distance vector routing. Proceedings of IEEE WMCSA, pp.90-100.

[19] Perrig, A., Stankovic, J. and Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), pp.53-57.

[20] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V. and Culler, D. (2002). SPINS: Security protocols for sensor networks. Wireless Networks, 8(5), pp.521-534.

[21] Roman, R., Zhou, J. and Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks. IEEE Consumer Communications and Networking Conference, pp.640-644.

[22] Sen, J. (2010). A survey on wireless sensor network security. International Journal of Communication Networks and Information Security, 1(2), pp.55-78.

[23] Sharma, S. and Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. ICTACT Journal on Communication Technology, 1(2), pp.42-45.

[24] Singh, S. K., Singh, M. P. and Singh, D. K. (2010). Routing protocols in wireless sensor networks. International Journal of Computer Science and Engineering Survey, 1(2), pp.63-83.

[25] Wang, Y., Attebury, G. and Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. IEEE Communications Surveys and Tutorials, 8(2), pp.2-23.

[26] Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. Computer, 35(10), pp.54-62.

[27] Xiao, B., Yu, B. and Gao, C. (2006). CHEMAS: Identify suspect nodes in selective forwarding attacks. Journal of Parallel and Distributed Computing, 67(11), pp.1218-1230.

[28] Yick, J., Mukherjee, B. and Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), pp.2292-2330.

[29] Yu, Z. and Cho, B. H. (2006). A trust model for wireless sensor networks. Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, pp.1-10.

[30] Zhang, Y., Lee, W. and Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), pp.545-556.