Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/53/20241424

Trust management systems in Wireless Sensor Networks

Xinyu Yue

School of Information and Communication Engineering, North University of China, Taiyuan, Shanxi province, 030051, China

2105034113@st.nuc.edu.cn

Abstract. The article begins by offering a comprehensive review of the current research landscape concerning trust management mechanisms. It elucidates the foundational concepts behind trust management mechanisms, subsequently detailing various attack models and the inherent vulnerabilities they exploit. A significant portion of the discussion delves into the primary computational methodologies employed in trust management. These encompass a range of techniques such as Bayesian statistics, subjective logic, fuzzy logic, D-s evidence theory, entropy theory, cloud theory, hierarchical analysis, fog computing, and machine learning. From this foundational understanding, the piece transitions to outline the challenges poised to shape the evolution of trust management mechanisms. This section not only emphasizes the hurdles currently faced by researchers and practitioners but also attempts to forecast the potential obstacles of the future. In culmination, the article encapsulates both the current state of research and the anticipated directions that promise to steer the trajectory of trust management mechanisms in forthcoming years. This holistic perspective aims to provide readers with a clear roadmap of the field's progression, emphasizing both its achievements and the milestones yet to be attained.

Keywords: Wireless sensor networks, Trust management, Secure transmission.

1. Introductory

Wireless Sensor Networks (WSNs) represent a paradigm shift in distributed wireless communication, primarily characterized by their self-organizing capabilities and extensive node distribution. These networks have become integral in various sectors, including military defense, medical monitoring, industrial operations, and the modernization of production processes. WSNs are renowned for their flexible networking abilities and suitability for large-scale deployments. However, they are not without limitations. Key constraints include limited node resources, restricted storage capacity, and a general inclination towards single-purpose network applications. Such limitations significantly impact the feasibility of traditional security encryption methods in WSNs, presenting challenges in defending against sophisticated and evolving attack models. The concern escalates in multi-domain environments where WSNs become particularly susceptible to various forms of attacks. These attacks, diverse in nature, tend to target different layers of the network architecture, disrupting standard node communication, and undermining trust collection and evaluation processes. One of the most concerning trends in WSN security is the increasing risk of node capture. This vulnerability stems from the network's limited ability to counteract only traditional forms of attacks. As the technology underpinning WSNs continues to evolve, the focus on securing trust management mechanisms grows

DOI: 10.54254/2755-2721/53/20241424

more critical. Trust management, rooted in the concept of trust, plays a vital role in supplementing traditional cryptographic methods. This approach to security is increasingly becoming indispensable in the quest to safeguard WSNs against the multifaceted threats they face in contemporary digital landscapes.

2. Trust management system

In their comprehensive analysis, Hong and Zhang present the fundamental components crucial to the architecture of a trust management system. These elements, integral to its operation, include: a specialized language for defining "behavior", a mechanism for identifying "subjects", a language tailored for articulating "security policies", and a system for the specification of "certificates" [1]. This framework is the bedrock upon which trust management systems are built, incorporating languages for the delineation of behavior and policies, a method for subject recognition, a standard for certificate definition, and a vital "consistency checker" for maintaining system integrity.

Expanding on this, Fang et al. delve into the operational aspects that are key to the functionality of a trust management system, namely: data collection, storage, modeling, transmission, and decision-making processes [2]. These aspects are interconnected and pivotal for effective node and data management. The collection process involves accumulating data to assess node reputation, including interaction statuses and sensory information from nodes. This process is underpinned by the principle that a more extensive range of collected data enhances the depth and accuracy of trust assessments.

The modeling phase is of paramount importance, as it shapes the trust and reputation framework within the system. This stage requires careful consideration of various factors such as the distribution of resource weights, strategies to counteract diverse threats, and the computational and resource demands of wireless sensor nodes.

Lastly, the decision-making process is based on the evaluated trust levels. This phase involves making critical decisions to penalize low-trust nodes and implement protective measures against internal threats. Conversely, nodes with higher trust ratings are prioritized for defense strategies against possible external attacks and vulnerabilities, ensuring a robust and secure network infrastructure, as illustrated in Figure 2.

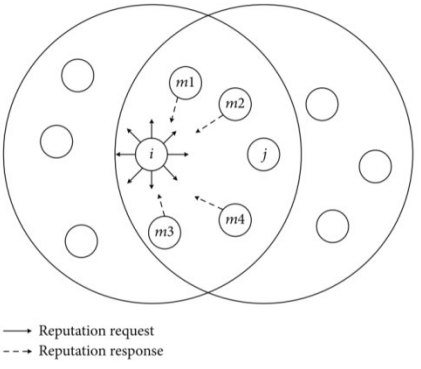

Figure 1. Process of reputation transfer [3].

DOI: 10.54254/2755-2721/53/20241424

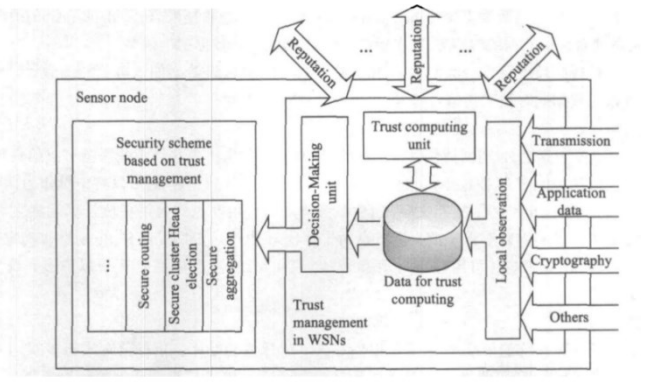

Figure 2. General architecture of trust management systems for WSNs [4].

3. Attack model

Various WSN environments exist that are susceptible to multiple levels and types of attacks. Trust management enhances the security of wireless sensors. However, challenges arise in minimizing energy consumption, simplifying design complexity, and combating the ever-evolving array of attack models. Addressing these challenges is pivotal for the advancement of trust management systems.

The inherent nature of wireless sensor networks makes each network layer vulnerable to distinct attacks. Predominantly, security concerns revolve around routing protocols. Malicious nodes can act independently, centrally, or in collusion. The adaptability and intricacy of colluding malicious node attacks, for which there are currently no robust defense mechanisms, warrant notable attention.

Attacks on the physical layer encompass physical sabotage, impersonation of captured nodes, signal jamming, eavesdropping, tampering, and node replication. The link layer often witnesses energy depletion attacks, link collision attacks, and non-equitable competition type attacks. A notable example of this category is the witch attack. In this, the attacker impersonates a node with multiple identities. When a route through this node gets compromised, another route with a distinct ID is selected. Due to the attacker's multiple identities in clustered networks, they exploit this mechanism, coercing surrounding nodes into their cluster domain to alter or discard regional node data. Malicious behaviors, such as packet dropping, address modifications, or packet content alterations, can be identified by inspecting trust elements [5, 6].

The transport layer is prone to flooding attacks, de-synchronization attacks, and information spoofing attacks. Attackers release false routes or impersonate base stations, altering routing information to divert network-wide communications to a specific locale, compromising the energy balance among sensors. Many evaluation models focus on basic metrics like the accuracy of forwarded packet content or the presence of malicious packet loss, making them vulnerable to intricate attacks. Trust management attacks indirectly diminish the reputation value of regular nodes or elevate that of malicious ones. A classic example is the malicious denigration attack, where attackers falsify the reputation value of genuine nodes, leading to trust conflicts [7].

Colluding attacks, representing typical conspiratorial assaults, require significant investment from the attackers but are incredibly challenging to detect and address. Multiple attackers collude, inflating each other's trust value, thereby confusing trust management systems. Their elusive nature makes them almost imperceptible to information management systems. Single attackers, too, employing sophisticated and adaptable techniques like switch attacks, pose a formidable challenge. In switch attacks, an individual attacker alternates identities to remain undetected, masquerading as a genuine node to gain high trust, especially when their actual trust value is low.

4. Trust Management Mechanism

In the realm of distributed trust management systems, the focus is on gathering and evaluating trust elements and node reliability data. This process involves intricate mathematical computations and

DOI: 10.54254/2755-2721/53/20241424

various analytical techniques to ascertain the trustworthiness of nodes, as outlined in Table 2. Traditional methods, such as Bayesian statistics, subjective logic, and fuzzy logic, are increasingly facing challenges in meeting the contemporary requirements of network trust assessment, especially in the context of big data. These traditional models, often characterized by a singular trust approach, exhibit limitations like high algorithmic complexity and slower operational speeds, making them less viable in today's rapidly evolving digital landscape [8, 9]. In contrast, newer technological paradigms like cloud computing, fog computing, and machine learning are gaining prominence. These technologies offer robust frameworks for processing and analyzing large volumes of data, aligning well with the needs of modern trust assessments. Their ability to handle big data efficiently positions them as more suitable candidates for trust evaluation in complex network environments. As a result, there's a noticeable shift towards leveraging these advanced computational techniques in trust management systems, recognizing their potential to offer more dynamic, scalable, and efficient solutions for assessing node trustworthiness in the era of big data [10-12].

5. Conclusion

This article commences with an introduction to the structure and operational steps of trust management mechanisms, followed by an in-depth analysis of the attack models and technical shortcomings of various trust management systems. While Wireless Sensor Networks (WSNs) boast portability and extensive coverage, they are also constrained by limited energy. These networks are susceptible to internal routing attacks, have limited defenses against certain types of attacks, and often lack rapid recognition speeds. Optimizing the trust mechanism can aid in identifying safe and energy-efficient routing paths, thus prolonging the network's life cycle without compromising security. However, addressing the varied attack models and managing resource consumption remain challenges that necessitate innovation in the trust computing system. Beyond the inherent adaptability of the trust model, issues with its uniformity and security deserve heightened scrutiny. The exploration of trust management offers a novel approach to resolving security issues. Investigating trust management mechanisms tailored to the unique attributes of wireless sensor networks holds significant research and practical implications. Yet, this approach also introduces challenges. Integrating the algorithms of trust management with the inherent features and limitations of the wireless sensors to enhance efficiency and defense capabilities remains a domain with myriad unresolved issues.

References

[1] Hong, F., & Zhang, Y. (2006). Research on trust management mechanism. Computer Applications, 26, 56-59.

[2] Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. Wireless Communications and Mobile Computing, 2020, 1-20.

[3] Qi, J., Liyong, T., & Zhong, C. (2008). Trust management in wireless sensor networks. Journal of Software, 19(7), 1716-1730.

[4] Jinfang, J., & Guangjie, H. (2020). Survey of Trust Management Mechanism in Wireless Sensor Network. Netinfo Security, 20(4), 12-20.

[5] Shuguang, Z., Qian, W., & Hao, W. et al. (2020). Sybil attack detection scheme based on AOA in heterogeneous wireless sensor networks. Journal of University of Science and Technology of China, 50(1), 72-78.

[6] Y J, H., H S, H., & M Q, Y. (2021). Trust-aware secure routing protocol for wireless sensor networks. Computer Engineering, 47(9), 145-152.

[7] Sun, B., & Li, D. (2017). A comprehensive trust-aware routing protocol with Multi-attributes for WSNs. IEEE Access, 6, 4725-4741.

[8] Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. ACM Trans Sens Netw (TOSN), 4(3), 15.

DOI: 10.54254/2755-2721/53/20241424

[9] Yao, Z., Kim, D., & Doh, Y. (2006). PLUS: Parameterized and localized trust management scheme for sensor networks security. 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), 437-446.
[10] Li, X., Zhou, F., & Du, J. (2013). LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf Foren Secur, 8(6), 924-935.
[11] Reddy, V. B., Negi, A., & Venkataraman, S. (2018). Trust computation model using hysteresis curve for wireless sensor networks. Proc. IEEE SENSORS, 1-4.
[12] Boubiche, D. E., Athmani, S., Boubiche, S., & Toral-Cruz, H. (2020). Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions. Springer Science + Business Media, LLC.