JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A ENERGY EFFICIENT TRUST AWARE ROUTING PROTOCOL IN WIRELES SENSOR NETWORK

[1]S.Boopathi, [2]Dr.A.Senthilkumar

[1]Guest Lecturer, , [2] Assistant Professor,

[1]Dept. of Computer Science, [2]Dept.of Computer Science,

[1]Government Arts College for Women,Nilakottai,Dindigul, Tamilnadu, India,

[2]Arignar Anna Govt.Arts College Namakkal-637002.

Abstract

We propose a trust-aware secure routing protocol (TSRP) with some new techniques to prevent attacks on wireless sensor networks. To counteract black hole, selective forwarding, wormhole, hello flood, and nodes first determine their neighbours' total trust values using direct trust value, indirect trust value, volatilisation factor, and residual energy. Second, in order to get data from one source node to another, that node must first send a routing request packet to its neighbours in multi-path mode. First, we examine typical attacks against trust-aware routing methods and their defining characteristics. After doing this analysis, unique proposals for both trust computation and trust derivation systems are made. Last but not least, we describe an improved routing method that makes use of both trust and quality-of- service measurements as routing indicators. Using simulations, we demonstrate that TSRF is capable of providing the desired level of security along with the high efficiency required by WSN-based networks. Through simulation, we see that TSRP outperforms ad hoc on-demand distance vector routing and a trust-based secure routing protocol in terms of network latency, packet loss rate, and average network energy usage.

Keywords – TSRF, WSN, Attacks, Energy Efficient Routing

1.Introduction

The widespread adoption of wireless sensor networks (WSNs) in a variety of settings, including defence, healthcare, manufacturing, urban planning, and transportation. However, the growth of WSNs is influenced by the limited computational power, storage capacity, energy, and other constraints of the nodes. It is especially easy for hostile nodes to launch routing attacks against WSNs when they are deployed arbitrarily in highly complicated systems. As a result, research into secure routing protocols for WSNs has become a hot topic in recent decades, and new approaches that can optimise security issues and reduce energy consumption in WSN are urgently needed. Malicious nodes, which are vulnerable to internal routing assaults because the attacker already knows all the key and passphrase information, are typically protected from external routing attacks by encryption and authentication-based security methods. In addition, these systems necessitate sophisticated calculations, which use more energy.

In this research, we offer a novel TSRP that takes into account both the direct trust value between a node and its neighbours and the indirect trust value decided by the common neighbours between the node and one of its neighbours. In addition, volatilization criteria are introduced to rapidly lower the previously high trust value of malicious nodes in order to eliminate them as soon as possible. Furthermore, assaults such as black holes, selective forwarding, hello floods, and sinkholes can be thwarted with the help of a holistic trust value that takes into account direct trust value, indirect trust value, and energy trust value. Finally, the sink chooses the best path to take based on the quality of the links and the number of hops involved in order to prevent wormhole attacks. Simulations are shown to assess how well TSRP performs in terms of average residual energy, throughput, end-to-end delay, packet loss ratio, and average comprehensive trust value.

Related works

Over the past few decades, numerous encryption-based systems have been developed to both extend network longevity and assure network security. Developed a system that combines online and offline cryptography to accomplish the goals of digital signature and encryption. The simulation results demonstrate that the packet transmission rate can be increased and the number of communication collisions can be decreased. It has a number of shortcomings, the most notable of which are its high computational complexity and the lack of clarity surrounding the types of attacks that may be defended against. The need for safe data transmission in clustering WSNs led to the introduction of a new encryption approach that relies on elliptic curve cryptography (ECC) and homomorphic encryption.

The paper details the types of attacks it can withstand, such as hello flood, denial of service, and compromised cluster head attacks. However, this approach causes a significant amount of delay and packet loss. As an additional line of defence against hello flood and selective forward-ing assaults, the ECC technique was employed to generate binary strings for each sensor, which were then utilised to form a unique 176 bit key. Not only is there less of a chance of packets being lost, but there is also less of a delay. However, when the method is run for 1000 rounds, the residual energy of each node fluctuates substantially, leading to uneven energy consumption; consequently, a new protocol based on ECC was proposed to speed up the authentication of multiuser message broadcasting. The protocol's four components—(a) system startup, (b) user addition, (c) multiuser broadcast authentication, and (d) user revocation—work together to accomplish secure data transmission. The computing cost of each node is reduced in part by enhancing the signature verification process. The outcomes demonstrate that the protocol's complexity and computing cost are drastically cut down. While the aforementioned encryption algorithms are useful, they are helpless against attacks coming from within the network itself. Accordingly, trust management- based secure routing protocols have been presented as a solution to the issues with the conventional encryption-based schemes, and a trust- based drone energy-saving data acquisition scheme has been proposed, which employs the quadratic optimization method of the drone path to determine routing paths. Trust inference and evolve procedures are also used to determine the sensor node's level of trustworthiness. That's why it's so efficient at locating the most productive path for gathering data and maintaining a consistent level of network activity while minimising overall power usage. For secure communication in WSNs while keeping power consumption low, the BRDT model makes use of the beta and direct trust paradigm. Too many cluster heads, however, waste energy because their communication ranges overlap. As BRDT did not detail which attacks could be defended against, a safe routing protocol based on the trust levels of nodes was developed, termed GradeTrust, to prevent black-hole attacks. Although GradeTrust has a higher packet delivery ratio, it can only protect against a black-hole attack. Therefore, a secure routing protocol based on clustering was proposed to protect against various assaults. To begin, we pick cluster leaders using a method that conserves power. Data confidence, data integrity, and comparison node assaults are only some of the numerous types of attacks that can be thwarted by encrypting it using a trusted hardware module as the network is in operation. A trust-based energy- preserving multihop routing protocol was presented, which is a mix of encryption and a trust management-based protocol. This addresses the issue of the cluster head nodes requiring permanent energy supply equipment, which results in stringent requirements for the WSN layout. The trust value of neighbour nodes is incorrectly calculated since it does not compute the indirect trust value. Therefore, a trust sensing se-cure routing mechanic was based on semiring theory. It optimises safe routing by taking into account the incentive factor, the energy trust, and the quality-of-service metrics, as well as the direct trust calculation of nodes and the indirect trust calculation of nodes. Powerful node computers are required. Therefore, a lightweight and easily deployable trust-based se-cure routing protocol (TBSRP) was proposed to lower the computational cost of the nodes and detect and isolate the misbehaving nodes. Ad hoc on-demand distance vector (AODV) routing is enhanced by this protocol, which allows for the selection of a path that is both trustworthy and efficient and that includes all trusted nodes. Some of AODV's most notable qualities are its ability to find routes on demand, its reduction of control packet overhead, its provision of up-to-date routing information, its ability to simultaneously broadcast and unicast routes, its low storage cost, its high scalability, and its quick connection establishment time. In addition, TBSRP automatically identifies malicious nodes to isolate them as soon as possible using a distributed trust paradigm. TBSRP can redirect a packet from the active path to a backup path if it meets a node with anomalous behaviour. The trust degree and hop number of nodes are utilised to choose the most reliable and shortest routing path. When computing the trust levels, however, it ignores the energy of the nodes, which could lead to the selection of nodes with high trust but low energy as the next hop.

1. Proposed Model

In this study, we assume a WSN containing n nodes is randomly distributed across a L m Mm rectangular region of interest, and that each node communicates with the sink by way of one of its neighbours.

Energy and Direct Model

Because their global trust values plummet due to the rapid decline of their previous trust values under the operation of the volatilization factors, hostile nodes executing black-hole attacks will be kicked out of the network. Furthermore, when hostile nodes initiate hello flood attacks, Rt values plummet to zero, and the nodes are subsequently eliminated due to their low comprehensive trust ratings. Similarly, the volatilization factors St and Rt can be used to protect against the damage that attacks like selective forwarding and sinkholes can do to a system's trustworthiness. Figure 5 compares the findings of an analysis of the average end-to-end delay. The average end-to-end delay of every method grows as the number of malicious nodes expands. Due to the lack of a defence mechanism, the packet loss rate in AODV rises precipitously as the number of rogue nodes grows. Once a packet is lost, the node must re- establish connection and retransmit the packets, which unavoidably lengthens the total transmission time. The average end-to-end delay for TBSRP and TSRP gradually rises with the number of rogue nodes, thanks to the protocols' built-in safeguards. On the other hand, TSRP has a much shorter latency than TBSRP.

Proposed Algorithm:

Input: Sample Data Transferred
Set: Dataset Testing area
TSRF Performance to the Given data
If Test is OK then
Analysis starts and do the next
else
Test again and again for the exact routing values
elifPreset values = settled Value
end if
Performing the TSRF for all Data Routing
Output: Threshold Data Expected

An Advanced TSFF with attacks

As a further measure of defence against word-of-mouth attacks, we also developed an inconsistency check scheme, which is depicted above. The bad-mouthers in the simulation either give a negative suggestion for good behaviour or a positive recommendation for poor behaviour. So, good behaviour (measured over a period of 30–70 seconds) amid bad mouth attacks results in a low trust value, and vice versa. The trust evaluation process may be affected more by more bad mouth attackers (percentage of bad mouth attackers = 0.5) than by fewer bad mouth attackers (proportion of bad mouth attackers = 0.25%). Because most erroneous recommendations are significantly different (higher or lower) from the ones offered by well-behaved nodes, our inconsistency check approach is able to filter out the vast majority of them. In conclusion, the proposed inconsistency check scheme can be used to increase the precision of trust evaluation. As we can see the proposed flow in detail in figure 1.

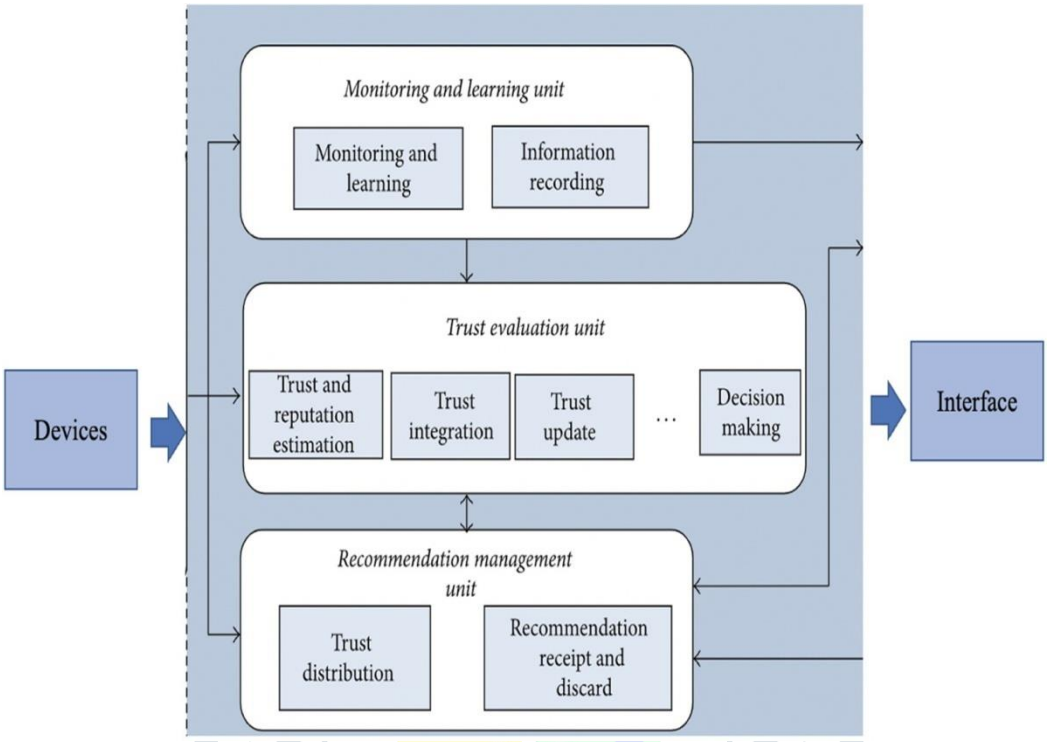
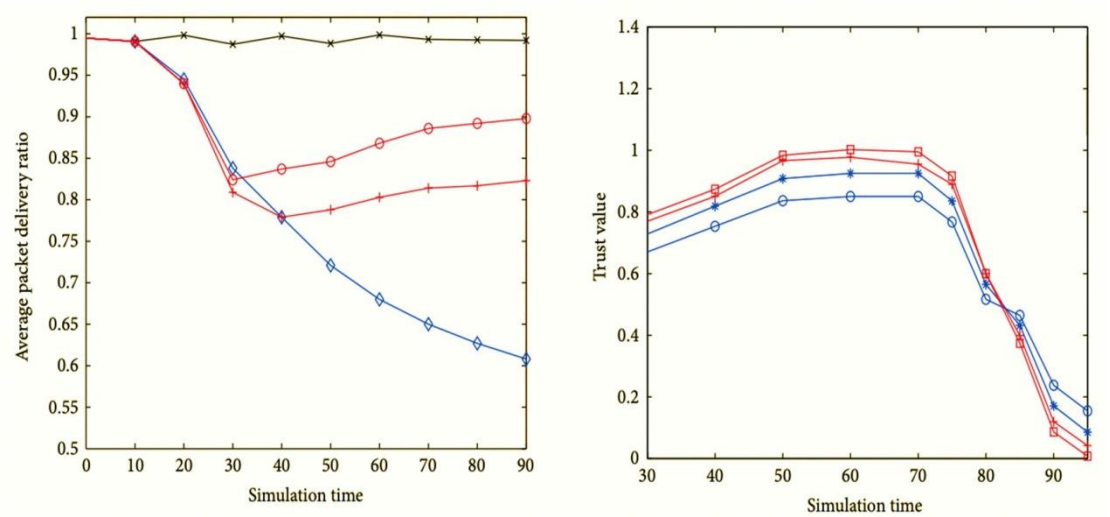


Figure 1. Proposed Flow

2. Evaluation Results

A node's level of safety is represented by its global trust value. A higher global trust value signifies tighter protection. Black-hole, hello-flood, sinkhole, selective-forwarding, and wormhole assaults are represented by attack1, attack2, attack3, attack4, and attack5, respectively, demonstrating the variation in the average comprehensive trust value of the malicious nodes under different attacks. When an attack is launched, 2% of malicious nodes are responsible. It demonstrates that the overall average trustworthiness of malicious nodes is falling. When a node's overall trust value drops below 0.35, the network considers it to be malevolent. Speeds at which TSRP identifies black-hole, hello-flood, sinkhole, and selective forwarding assaults are shown in the figures to be 12%, 5%, 10%, and 5.3% faster than the values for TBSRP.

Figure 2. Test 1



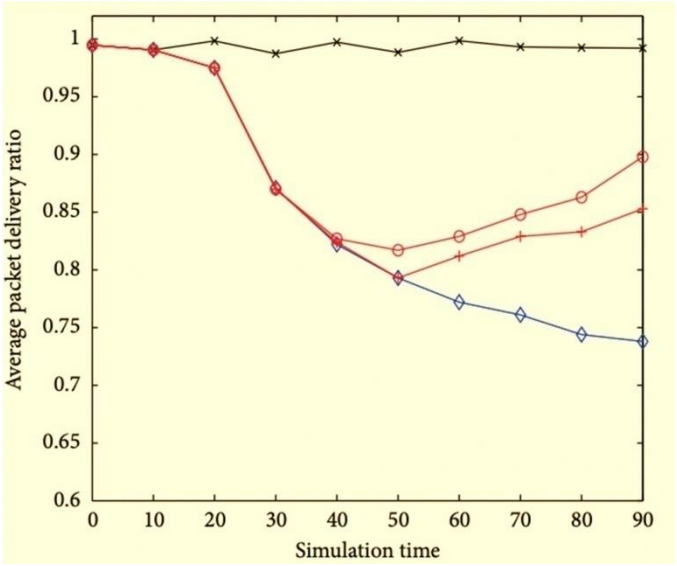


Figure 3. Test 2

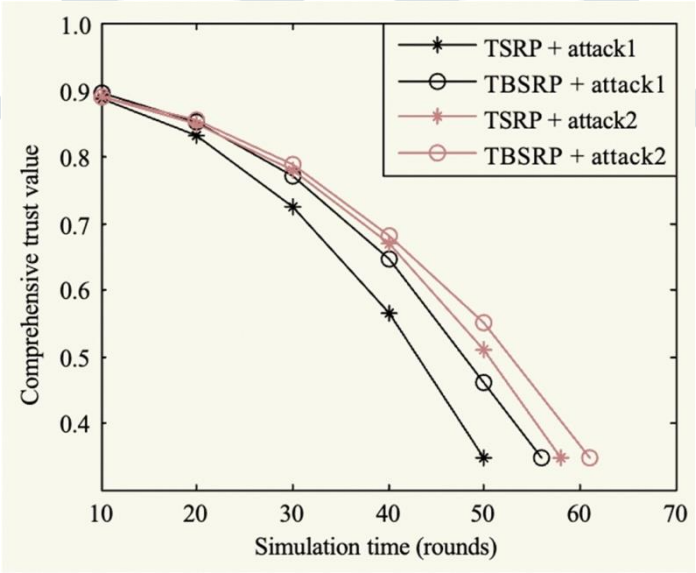


Figure 4. Test 3

The direct trust value of malicious nodes soon drops because TSRP considers the role of historical trust values and volatilization factors when calculating direct trust values. As shown in Figure, TBSRP is helpless against a wormhole assault, while TSRP can swiftly filter out malicious nodes that launch wormhole attacks because, in TSRP, the sink evaluates the link quality to exclude a link implicated in the wormhole attack from the network in the routing establishment phase. Therefore, in the case of malicious attacks, TSRP can swiftly lower its trust value and exclude it from the network, rendering it incapable of participating in any network activities.

3. Conclusion

Reliable and energy-efficient data transmission is difficult because nodes' behaviours are dynamic and unpredictable. The purpose of this study was to propose TSRP, a trust-aware safe routing protocol. To counteract black holes, selective forwarding, hello floods, and sinkholes, we suggested a lightweight trust computation and trust derivation system called TSRP, which takes into account a node's direct trust value, indirect trust value, volatilization factor, and residual energy. The simulation findings demonstrated that TSRF had a broader range of applicability and may increase network performance under the assumption of security assurance, particularly in dense networks, when compared to some conventional trust-ware approaches. To prevent wormhole attacks and conserve energy during the optimal path search and data transmission, the sink then chooses a routing path with good security and minimal hops. It is clear from the simulation findings that TSRP was able to accomplish its goal of secure, energy-efficient data transmission. In addition, TSRP outperforms AODV and TBSRP in terms of mean throughput, average end-to-end delay, mean comprehensive trust value, and mean packet loss rate.

References

1. Abualkishik, A. Z., &Alwan, A. A. (2022). Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks. *Journal of Cybersecurity and Information Management*, *9*(1), 40-51.

2. Dinesh, K., & SVN, S. K. (2022). Trust Aware Secured Energy Efficient Rule based Fuzzy Clustering Protocol with modified Sun Flower optimization Algorithm in Wireless Sensor Networks.

3. Rajan, D. P., Premalatha, J., Velliangiri, S., & Karthikeyan, P. (2022). Blockchain enabled joint trust (MF-WWO-WO) algorithm for clustered-based energy efficient routing protocol in wireless sensor network. *Transactions on Emerging Telecommunications Technologies*, e4502.

4. Usturge, S., & Pavan Kumar, T. (2022). DEroute: trust-aware data routing protocol based on encryption and fuzzy concept for MANET secure communication in Iot. *Information Security Journal: A Global Perspective*, 1-16.

5. Joselin, J., & Sofia, V. A. A security Trust Mechanism for Transferring Packets to Sink Node in Wireless Sensor Networks.