A LIGHT-WEIGHT TRUST AWARE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Adnan Ahmed[1], Khalid Haseeb[2] & Sohail Khokhar[3]

[1]Department of Computer Systems, Quaid-e-Awam University, Nawabshah
[2]Department of Computer Science, Islamia College, Peshawar, Pakistan
[3]Department of electrical Engineering, Quaid-e-Awam University, Nawabshah

ABSTRACT

The interest of research community has significantly increased in wireless sensor networks during last few years due to low-cost solutions for wide range of applications. Most of the times sensor nodes in WSN operate unsupervised which exposes them to variety of security threats, particularly node misbehavior attacks. Therefore, secure data dissemination becomes a challenging task due to unpredictable behavior of nodes. Most of the trust aware routing protocols exclusively focus on identification and isolation of misbehaving nodes over multihop path. However, these schemes do not optimize the route formation by considering important characteristics like path length and energy resources. As a result, these existing schemes exhibits compromised route stability and network lifetime. This paper presents a light-weight trust aware routing protocol that dynamically detects and isolate misbehaving nodes and paves the way for trusted environment. Proposed LTRP scheme employs a multi-facet routing metric integrating node's trust, energy and hop counts for making routing decisions. Simulation based performance evaluation reveals improved network lifetime, throughput, delay, and routing load performance of LTRP when compared to state-of-art.

Keywords: *Security, Trust, Routing Node Misbehavior Attack*

INTRODUCTION

WSN is an emerging technology that has revolutionized the people's interaction with surrounding environments with availability of smart sensor nodes. The sensing, computing and short-range communication capabilities of sensor nodes make them suitable to be deployed in variety of applications like battle field monitoring, environmental monitoring, vehicle tracking, health applications and disaster response operations (Pilloni & Atzori 2011). The deployed sensor nodes may be exposed to physical capture and variety of attacks (particularly node misbehavior attacks) due to unsupervised nature of environment in which they operate. A misbehaving node may inject false information to data packets, misroute the data packets and in worse scenario may intentionally drops packets to disrupt the communication. Such communication disruption results in significant loss of critical information and undermines the benefits of such networks. Several secure solutions based on traditional cryptographic primitives have been develop (Haque, Mokammel, Pathan,

Hong & Huh, 2008; Hu, Perrig & Johnson 2005) to protect WSN against variety of attacks.

However, these schemes assume that all nodes are trusted entities and cooperate in packet forwarding. Whereas, this assumption is not true as nodes change behavior dynamically, therefore, these schemes are not capable of defending against node misbehavior attacks (Momani & Challa 2010). Furthermore, the applicability of these schemes is limited to resources constrained WSN as these schemes require high processing, computations, energy and memory resources (Cordasco & Wetzel 2008). Trust based schemes have been designed to tackle node misbehavior attacks, in order to overcome limitations of traditional schemes. Trust based schemes facilitates in identification of misbehaving nodes based on their past actions. However, most of existing trust aware schemes exhibits vulnerabilities when comes to handle node misbehavior attacks. Most of the schemes designed for mobile ad hoc networks (Cho, Swami & Chen, 2012; Eissa, Tameem, Razak, Khokhar & Samian, 2013; Wang, Chen & Chang 2014) cannot directly applied to resource constrained sensor network, as mobile ad-hoc networks have sufficient resources like battery, processing and storage.

Similarly, existing trust aware routing approaches (Channa & Ahmed 2011; Duan, 2014; Qu, 2013; Wang, Chen & Chang 2014) do not focus on optimizing end-to-end route keeping in view the resource limitations of sensor nodes. Therefore, trusted nodes depletes their energy in quick fashion thereby leads to high number of dead nodes in network which not only compromises overall lifetime of the network but also results in the storm of route discoveries. Though, most of existing trust aware schemes exhibits vulnerabilities when comes to handle node misbehavior attacks. In addition, non-optimize route selection may also result in longer path selection. Longer paths have high probability of failure; cause more delays and requires more retransmissions (Zadin & Fevens 2013). Moreover, most of the existing schemes (Duan, 2013; Leligou, 2012) exhibit high overheads (communication and computational) due to extensive computational operations involved in trust estimation and dissemination.

This paper presents a new Light-weight Trust aware Routing Protocol (LTRP) for WSNs that aims to provide optimized route selection by keeping in view aforementioned limitations. In order to avoid the pre-mature energy depletion of trusted node, LTRP incorporates residual energy based threshold mechanism in route selection which helps to prolong the network lifetime. LTRP basically uses a composite routing metric which is calculated based on three factors: trust level, residual energy, number of hops. The net-effect of the composite routing function is to select the shortest route comprised of trusted and energy-efficient nodes. The designed composite metric for LTRP also helps the trusted nodes to balance the load more efficiently. The remaining of paper is structured as follows:

Section II presents the related literature review of existing trust aware routing schemes. The proposed LTRP scheme is discussed in detail in Section III. Section IV presents the simulation based performance evaluation of LTRP scheme. Finally, section V concludes the paper.

LITERATURE REVIEW

Several trust aware routing schemes have been developed for senor and ad-hoc networks, over years. A trust aware routing protocol has been proposed for sensor actuator network (Rezgui & Eltoweissy 2007). The parameters like echo ratio and link quality have been used for evaluating the trustworthiness. The echo ratio represents broadcast overhearing messages in promiscuous mode. TARP makes use of various broadcast and unicast messages for maintaining and updating link quality, communication state and echo ratio. However, the type of node misbehavior attacks and its effect on trust model is neither mentioned nor considered. The link quality parameter for evaluating trust is not an appropriate choice as link quality may degrades due to inference or noise which affects the decision making capability of trust model. Also, efficacy of proposed scheme is only measured in term of energy consumption which is not the relevant parameter for evaluating the efficacy of trust based scheme. Wang et al. proposed a Trust based QoS routing scheme (Wang, Chen & Chang 2014) for mobile ad-hoc networks that employs both direct and indirect trust for evaluating trustworthiness of neighboring nodes.

Trust-based QoS model of TQR make use Expected Transmission Count (ETX) for measuring link quality by exchanging probe packets (one probe broadcast every second). TQR preserved adjacencies with neighboring nodes through periodic exchange of Hello packets. Though, proposed TQR scheme detects and isolates misbehaving nodes, however incurs high overheads in trust estimation and disseminations. The frequent exchanging of Hello and probe packets lead to high network loads. Moreover, no mechanism is provided to prevent false recommendations from a misbehaving node. A Reliable AODV (R-AODV) (Channa & Ahmed 2011) scheme is proposed for mobile ad hoc networks to detect misbehaving nodes in network. The packet forwarding ratio is summed up for evaluating node's trust rating. The trust estimation involves only direct observation of nodes. R-AODV overlook optimize route discovery by taking care of remaining energy of nodes thereby increases the probability of dead nodes. Moreover, the trust convergence takes considerable amount of time as R-AODV relies on direct trust only. Thus, misbehaving nodes remain part of active route for more time.

Tajeddine et al. proposed a CENtralized Trust-based Efficient Routing protocol with an appropriate Authentication (CENTERA) (Tajeddine et al. 2015) which consists of a central Base Station (BS) that evaluates the trustworthiness of every node based on their packet

forwarding ratio. In addition to concept of trust, CENTERA exploits traditional security mechanisms such as cryptography and Message Authentication Code (MAC) for necessary validation of nodes and generated packets. While CENTERA can counter impersonating, modification and reply attacks but cannot completely defend against node misbehavior attacks. Still, it carries out encryption and decryption at each intermediate node during the route discovery, which significantly increases the computations, energy consumption, and network overheads thus compromising node's energy reserve. The centralized trust management schemes are less reliable as they are vulnerable to single point of failure or result in collapsing the entire network if BS is compromised. A Trust Aware Routing Framework (TARF) scheme (Zhan, Shi & Deng 2012) has been proposed for WSN to deal with wormhole attacks. The trust and energy cost values are stored by each node for their known neighbors.

TARF employ asymmetric authentication scheme for verifying broadcast packets, which requires a cryptographic algorithm and time synchronization. However, frequent exchange of cryptographic keys and energy control packets increases memory requirements and overheads. TARF do not optimize route selection, therefore, selected route may not meet requirements for trusted and energy efficient routing. Furthermore, TARF imposes several constraints such as asymmetric authentication and synchronization for network operations thereby limit the scope for resource constrained WSN. It is observed from the presented literature that most of the existing trust aware does not optimize the end-to-end route by keeping in view trust, energy and path length. Moreover, it is also observed that trust and energy awareness has gained little attention, and still a light-weight, trust and energy aware scheme is required which neither requires any specialized information (geographic information or asymmetric authentication) nor imposes too many constraints (tight time synchronization).

The paper, as main contribution, presents a light weight trust aware routing protocol that optimizes the route selection by considering critical design parameters for reliable and efficient routing such as trust, energy, and path length.

PROPOSED LTRP SCHEME

This section presents the detailed discussion of our proposed scheme LTRP. LRTP is extension of our previous work (Ahmed et al. 2015) to integrate concept of trust and energy awareness. The certain assumptions need to be clarified before presenting the detailed design of LTRP scheme: A misbehaving node sends fake route reply packets so that it may become part of active route. Once misbehaving node becomes part of active route it drops all the received packets. The packet forwarding behavior of neighboring nodes is monitored using promiscuous mode. The source and destination nodes are assumed not to be

compromised.

Design of Proposed LTRP Scheme

The design of LTRP scheme based on trustworthiness and energy efficiency, as a result LTRP consist of two major phases: Trust Evaluation and Trust-Energy aware Routing. The Trust Evaluation phase is responsible for providing trusted network environment by identifying the misbehaving nodes. The energy awareness is incorporated in trust-energy aware routing phase which is responsible for providing optimized routes in terms of trust, energy, and hop count.

Trust Evaluation

The trust evaluation phase estimates the degree of trustworthiness of nodes by monitoring the packet forwarding behavior in promiscuous mode (Marti et al. 2000). Both direct and indirect trusts are used to evaluate total trustworthiness of nodes. A node evaluates the direct trust by its own observations for packet forwarding behavior, whereas indirect trust is gained through recommendations provided by other nodes for a particular node. A buffer is maintained by each sensor node to store necessary information being used in trust estimation such as next-hop identification, packet identification number, sender, and receiver IDs. The packet forwarding behavior of node j, helps node i to evaluate trust rating for node j represented by $T_{i,j}$ as in equation (1).

$$T_{i,j} = w_1 \times T_{i,j}\text{Direct} + w_2 \times T_{i,j}^{k}\text{Indirect} \quad (1)$$

The direct trust node i has for node j is represented by $T_{i,j}\text{Direct}$. The degree of indirect trust that node i has learned from its neighbors is denoted by $T_{i,j}^{k}\text{Indirect}$. The w_1 and w_2 are weight factors assigned to $T_{i,j}\text{Direct}$ and $T_{j,k}\text{Indirect}$ respectively, such that $w_1 + w_2 = 1$, whereas $0 \leq w_1 \leq 1$ and $0 \leq w_2 \leq 1$. The direct trust, $T_{i,j}\text{Direct}$ in equation (1), is evaluated by estimating the packet forwarding ratio as shown in equation (2).

$$T_{i,j}\text{Direct} = \sum_{p=0}^{N-1} \text{Forwarded}\ (p) \Big/ \sum_{p=0}^{N-1} \text{Received}\ (p) \quad (2)$$

An indirect trust in gained recommendations provided by neighbors about their own interactions. The indirect trust $T_{i,j}(t)$ is evaluated as:

$$T_{i,j}^{k}\text{Indirect} = \frac{1}{n} \sum_{k=1}^{n} T_{k,j} \quad (3)$$

$T_{k,j}$ represents the indirect trust evaluated by common of neighbors of node i that are node j and node k. $T_{k,j}$ is the average of trust evaluated by neighbors of node i (node k) for node j. The trust convergence is speed-up by incorporating indirect trust in trust estimation.

If the trust rating of a node is above specified threshold γ, the node is considered as trusted node, otherwise it is considered as misbehaving node. The output of trust evaluation phase when combined with route discovery phase helps in selecting trusted and energy-efficient routes.

Trust-Energy Aware Routing

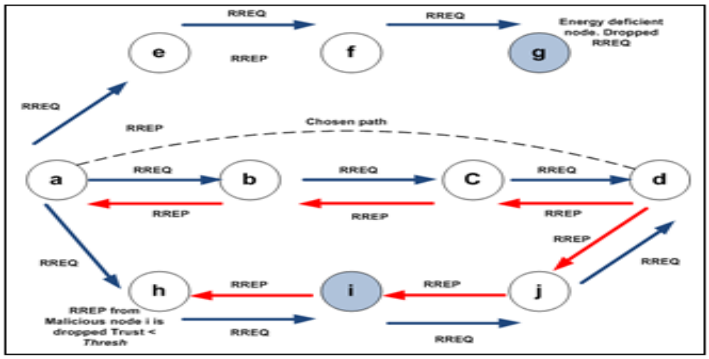
The Trust-Energy aware routing is responsible for establishing shortest, energy-efficient, and trusted routes. The proposed LTRP scheme expands the route setup process of AODV. The LTRP customizes the default RREQ and RREP control packets of AODV for selecting trusted, energy efficient and shortest routes in route discovery phase. For achieving this goal, LTRP incorporates a Routing Function (RF) metric, as shown in the equation (4), which includes nodes' trust, remaining energy and hop counts.

$$RF = x * \text{trust level} + y * \text{remaining energy} + z * \text{Hop count} \quad (4)$$

The x, y and z represent the impact (weight) of trust, energy and hop count respectively, in route selection such that $x + y + z = 1$. The RF facilitates the selection of route that passes through trusted, energy efficient and shortest path thereby results in improved throughput, lifetime and route stability performance. The trusted nodes whose energy level is above threshold (20% of initial energy reserve) are selected to route the packets. When a source node broadcasts a Route Request (RREQ) packet, every intermediate node that receives it appends its own remaining energy in packet header as well as number of hops traversed so far. If energy level is below specified threshold, route request packet is dropped, as shown in Figure 1. The node g drops the RREQ as it does not have enough energy resources to participate in packet forwarding.

When destination receives the RREQ packet, it inserts trust level and hops field in Route Reply (RREP) packet and sends back to source node. On its way back, upstream node receiving the route reply packet checks whether the downstream node which has forwarded the RREP packet has sufficient trust degree value. If trust value is below threshold, the RREP packet is discarded; otherwise trust level of downstream node is added to RREP packet header and forwarded to upstream node. As shown in Figure 1, the RREP packet from node i is dropped by node h, as node i has trust rating below specified trust threshold. Same procedure is repeated till the RREP packet reaches source node. The source then makes final decision by calculating the routing cost of all the routes by using trust, energy, and hop count. The optimized route in terms of trustworthiness, remaining energy level, and hop count value is selected for packet forwarding which results in less interference and fewer retransmissions.

Figure 1: Route selection using LTRP



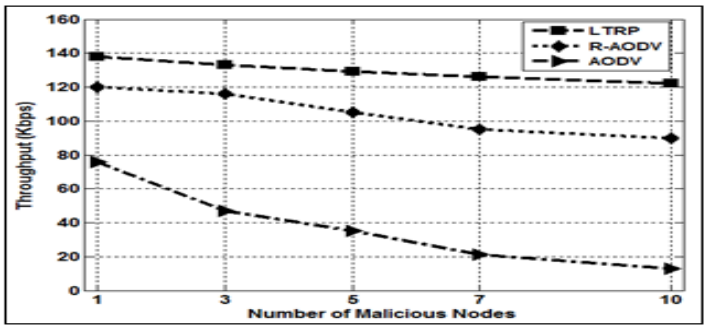
RESULTS AND DISCUSSION

Network Simulator-2 has been used to evaluate the performance of LTRP scheme using the simulation parameters listed in Table 1. Figure 2 presents performance evaluation of three schemes in terms of throughput. LTRP exhibits improved throughput performance as compared to AODV and R-AODV due to its adopted methodology in trust evaluation and optimized route selection. Integrated concept of energy efficiency and trust contributes to selection of trusted and energy efficient routes thereby packets flow remains consistent for more time period. But, R-AODV do not pay attention to remaining energy levels of nodes, thus results in high number of dead nodes which brings drastic impact on throughput performance. Similarly, slow trust convergence in R-AODV allows the misbehaving nodes to drop more number of packets which also bring down the throughput. The throughput performance of AODV is significantly reduces as it does not have capability to counter misbehaving nodes. So, they get opportunity to drop high number of data packets freely.

Table 1. Simulation parameters

Parameters	Values
Network area	1000 m x 1000m
Simulation time	1000 sec
Number of nodes	100
Number of misbehaving nodes	1 – 10
Initial Energy	50J
Energy Threshold (ε_{thresh})	20% of initial energy
Trust Threshold (δ)	0.6
Transport layer protocol	UDP
MAC Layer protocol	IEEE 802.15.4
Network Layer protocol	LTRP, R-AODV, AODV
Traffic type	CBR
Packet size	1500 bytes
Weight for direct trust w_1	0.7
Weight for indirect trust w_2	0.3
RF weights (x, y and z)	0.333

Figure 2. Throughput performance



The network lifetime performance of LTRP, AODV and R-AODV is shown in Figure 3. In AODV most of the nodes in the network are not involved in packet forwarding because misbehaving nodes capture the packets and drops them. As a result, energy reserves for most of the nodes remains intact thereby exhibits improved network lifetime. However, it brings down the throughput performance. The nodes in R-AODV exclusively focus of selecting trusted routes without taking care of energy resources thereby leads to quick energy depletion on the part of trusted nodes which consequently results in compromised network lifetime. However, the design of LTRP focuses on trustworthiness and energy efficiency thereby allows the trusted node to balance the load on the basis of residual energy, if it feels that its energy level reached to threshold.

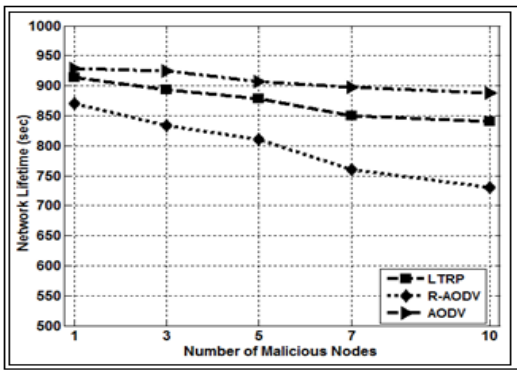


Figure 3. Network lifetime performance

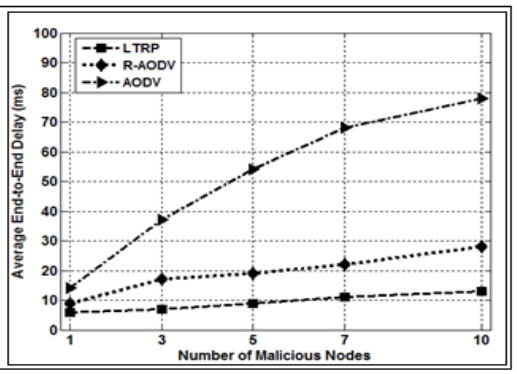


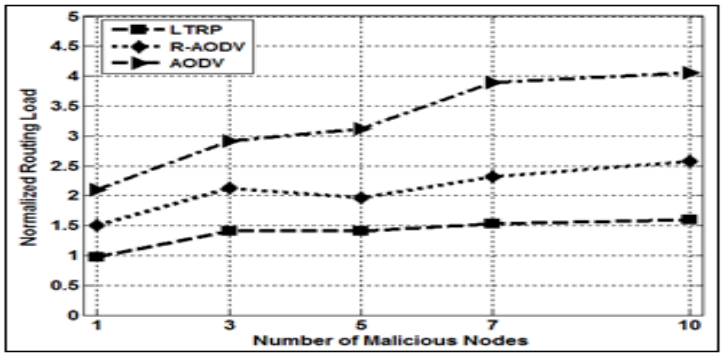
Figure 4. Average Delay performance

Figure 4 shows the end-to-end delay performance of three schemes. The optimized route selection mechanism of LTRP enables to find shortest, trusted and energy efficient routes which bring significant impact on delay performance as packets have to travel from shortest path to reach destination. Whereas, AODV and R-AODV select longer paths once shortest routes are not available due to misbehaving or dead nodes on active route. Therefore, it results in high number of route breakages thereby results in high delay till new routes are

discovered. The end-to-end delay performance for AODV significantly reduced as least number of packets reaches destination due to high number of packets dropped by undetected misbehaving nodes on active route.

The Normalized Routing Load (NRL) performance for three schemes in presented in Figure 5. LTRP outperforms AODV and R-AODV as it selects stable and trusted routes thereby requiring less retransmissions and interference on links. However, R-AODV exhibits high routing load due to increased number of route discoveries and route maintenance calls and it shows the NRL performance of all three schemes. In AODV, undetected misbehaving nodes create disconnection in most part of network as a result drop ratio is significantly increased. Consequently, results in increased number of retransmissions which contributed to high routing load.

Figure 5. Network Routing Load performance



CONCLUSION

In this paper, we proposed a readily deployable Light-weight Trust aware Routing Protocol (LTRP) for wireless sensor network to detect and isolate misbehaving nodes. The simulation results prove the efficacy of proposed LTRP scheme. The performance of LTRP is compared against AODV and R-AODV about average end-to-end delay, throughput, NRL and network lifetime. The simulation results show that misbehaving nodes badly affect the overall performance of AODV and bring down the performance metrics to unacceptable ranges. LTRP significantly improves the overall network performance and isolates misbehaving nodes at earliest. As part of future work, we plan to compare the performance of proposed scheme against other node misbehavior attacks such as wormhole and Sybil attacks.

References

Adnan, A., Bakar, A. K., Channa, M., & Haseeb, K. (2015). Countering Node Misbehavior Attacks Using Trust Based Secure Routing Protocol. *Telkomnika: Telecommunication Computing*

Electronics and Control, 13(1): 260–68.

Channa, M. I., & Ahmed, M. K. (2011). A Reliable Routing Scheme for Post-Disaster Ad Hoc Communication Networks. *Journal of Communications*, 6(7): 549–57.

Cho, J., Swami, A., & Chen, I. (2012). Modeling and Analysis of Trust Management with Trust Chain Optimization in Mobile Ad Hoc Networks. *Journal of Network and Computer Applications* 35(3), 1001–12.

Cordasco, J., & Wetzel, S. (2008). Cryptographic Versus Trust-Based Methods for MANET Routing Security. *Electronic Notes in Theoretical Computer Science*, 197(2), 131–40.

Duan, J. (2014). TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, 1–14.

Duan, J., Deyun, G., Chuan, H. F., & Zhang, H. (2013). TC-BAC: A Trust and Centrality Degree Based Access Control Model in Wireless Sensor Networks. *Ad Hoc Networks*, 11(8), 2675–92.

Eissa, T., Shukor, A. R., Rashid, H. K., & Samian, N. (2013). Trust-Based Routing Mechanism in MANET: Design and Implementation. *Mobile Networks and Applications* 18(5), 666–77.

Haque, M. M., Pathan, A. K., Hong, C. S., & Huh, E. (2008). An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks." *KSII Transactions on Internet and Information Systems*, 2(5), 265–79.

Hu, Y., Adrian, P., & Johnson, D. (2005). Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*, 11(1-2), 21–38.

Leligou, H. C. (2012). Combining Trust with Location Information for Routing in Wireless Sensor Networks. *Wireless Communications and Mobile Computing*, 12(12), 1091–1103.

Marti., T. J.. Giuli, K. L., & Baker, M. (2000). Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, New York, New York, USA: ACM, 255–65.

Momani, M., & Challa, S. (2010). Survey of Trust Models in Different Network Domains. *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, 1(3), 1–19.

Pilloni, V., & Atzori, L. (2011). Deployment of Distributed Applications in Wireless Sensor Networks. *Sensors*, 11(8), 7395–7419.

Qu, C. (2013). Light-Weight Trust-Based On-Demand Multipath Routing Protocol for Mobile Ad Hoc Networks. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Ieee, 42–49.

Rezgui, A., & Eltoweissy, M. (2007). TARP : A Trust-Aware Routing Protocol for Sensor-Actuator Networks. In *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS)*, 1–9.

Tajeddine, A. (2015). Centera: A Centralized Trust-Based Efficient Routing Protocol with Authentication for Wireless Sensor Networks. *Sensors*, 15(2), 3299–3333.

Wang, B., Xunxun, C., & Chang, W. (2014). A Light-Weight Trust-Based QoS Routing Algorithm for Ad Hoc Networks." *Pervasive and Mobile Computing*, 13, 164–80.

Zadin, A., & Fevens, T. (2013). Maintaining Path Stability with Node Failure in Mobile Ad Hoc Networks." *Procedia Computer Science*, 19, 1068–73.

Zhan, G., Weisong, S., & Julia, D. (2012). Design and Implementation of TARF : A Trust-Aware Routing Framework for WSNs." *IEEE Transactions on Dependable and Secure Computing*, 9(2), 184–97.