Countering Node Misbehavior Attacks Using Trust Based Secure Routing Protocol

Adnan Ahmed[1], Kamalrulnizam Abu Bakar[1], Muhammad Ibrahim Channa[2], Khalid Haseeb[1]
[1] Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310, Johor Bahru, Malaysia.
[2] Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, 67450, Pakistan.
e-mail: adnan.ahmed03@yahoo.com[1], knizam@utm.my[1], ibraheem_channa@yahoo.com[2], khalidutm.pcrg@gmail.com[1]

Abstract

Wireless sensor networks have gained remarkable appreciation over the last few years. Despite significant advantages and tremendous applications, WSN is vulnerable to variety of attacks. Due to resource constraint nature of WSN, applicability of traditional security solutions is debatable. Although cryptography, authentication and confidentiality measures help in preventing specific types of attacks but they cannot safeguard against node misbehavior attacks and come at significant cost. To address this problem, we propose a Trust Based Secure Routing Protocol (TBSRP) which relies on distributed trust model for the detection and isolation of misbehaving nodes. The TBSRP aims to establish shortest path that contain all trusted nodes, identify packet forwarding misbehavior caused by malicious and faulty nodes and reroute the traffic to other reliable paths. The performance of TBSRP is evaluated in terms of packet delivery ratio, average end-to-end delay and normalized routing load. Simulations results show that TBSRP can achieve both high delivery ratio and throughput in presence of various numbers of misbehaving and faulty nodes.

Keywords*: trust, wireless sensor networks, security, node misbehavior, faulty nodes*

1. Introduction

The interest of research community has significantly increased in sensor networks during last few years due to low-cost solutions for diversity of applications including environmental monitoring, vehicle tracking and detection, healthcare, traffic control in smart roads, battle field monitoring, surveillance and battle damage assessment [1]–[3]. Most of the times WSN operates in un-attended environments which exposes the deployed sensor nodes to variety of security attacks [4],[5]. The security attacks in WSN may be classified into two types: *Outsider (External) attacks* and *Insider or node misbehavior attacks* [6]. In outsider attack, attacker lacks authentication and key information and such type of attack can easily be dealt with classical security mechanism such as cryptography, encryption and authentication. In insider attack, an adversary already has all key and cryptographic information so that it can easily change the behavior of a node. Therefore, such type of node misbehavior attacks cannot be dealt with traditional security measures. The most common insider attacks are wormhole, blackhole, selective forwarding and sinkhole attacks [7]–[9]. Several secure solutions have been develop [10]–[12] to protect WSN against variety of attacks. However, these solutions exploit traditional security mechanisms such as cryptography and authentication which are mostly not suitable to counter nodes' misbehavior attacks as these techniques assume that participating nodes as cooperative and trustworthy. However, this assumption is not realistic for insider or node misbehavior attacks [13]. Similarly, these traditional security measures require some sort of central administration for security management which is usually not available in self-organized ad-hoc and sensor networks [14]. The efficacy of cryptography based solutions is ineffective in a case where an authorized compromised sensor node due to internal attack, can have easy access to memory contents and valid secret keys [15]. In addition, these traditional security solutions require high computation, memory and energy consumption which restrict their implementation in resource constrained sensor nodes [16].

To overcome limitations of traditional security primitives, the concept of trust has been successfully applied to ad-hoc and sensor networks to counter node misbehavior attacks. Trust

Received September 28, 2014; Revised December 12, 2014; Accepted January 6, 2015

management is an effective tool that is suitable for security architecture of sensor network [17],[18]. Several trust aware routing schemes have been developed over the years. In [19] a geographical trust aware routing protocol for combating blackhole and grayhole attacks in sensor network is proposed, which however generate huge amount of traffic over network by sending periodic updates for collecting firsthand (direct) and secondhand (indirect) information. Moreover, if the node mobility is very high it may increase trust build-up mechanism time. To defend against wormhole attack in WSN, a trust-aware routing framework (TARF) has been proposed [20]. Each node to keeps record for trust and energy cost values for their known neighbors. Trust evaluation is based on detecting routing loops, whereas nodes involved in routing loops are penalized. Energy control messages are broadcasted that contains energy cost information to deliver a packet. However, broadcasting of energy control packets may increase routing load and it may also suffers from selfishness attack where a compromised node may send false energy cost information. A trusted node may be declared as malicious node if it drops packets due to significant level of congestion. In [21] trust based routing protocol based on AODV (TAODV) is proposed for MANET which exploits trust information in route discovery. The proposed scheme is not feasible for resource constrained environment such as WSN as it is computationally intensive and makes use of cryptographic module for providing security. Furthermore, authors did not consider the effects of attacks on their proposed scheme. A trust aware routing protocol (TARP) has been proposed for sensor actuator network [22]. 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 effects in the decision making capability of trust model. Furthermore, 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. In [23], a trust based routing scheme, Friendship based AODV (Fr-AODV), is presented to counter blackhole attack. Trust evaluation is based on certain features such as node reputation and node identity. Each feature is assigned attribute number that is exchanged during packet forwarding. However, the proposed solution is not completely robust against node misbehavior attacks. The authenticated compromised node may exchange false information such as feature attribute number which may lead to incorrect decision making by trust model. Moreover, Fr-AODV is vulnerable to wormhole attack where a malicious node impersonates its identity. The increased number of route maintenance calls and exchange of hello messages also increases load on trusted nodes.

In this paper, we propose a light weight and quickly deployable Trust Based Secure Routing Protocol (TBSRP) for WSN to detect and isolate misbehaving and faulty nodes. TBSRP employ distributed trust model for dynamic identification of malicious and faulty nodes and thereby isolates them at earliest. TBSRP can re-route the packets to alternate routes if active paths encounter faulty or misbehaving nodes. The node's trust level and hop count are used for selecting reliable and shortest route. The rest of this paper is organized as follows. Section 2 provides proposed TBSRP scheme. Section 3 presents the research methods. Section 4 presents the simulation results and section 4 concludes the paper.

2. TBSRP- Proposed Scheme

The routing in WSN is modeled as directed graph $G = (V, E, W)$ where V represents set of sensor node in network, E represents the set of links between the nodes and W represents the metrics used for measuring links. A trusted path P consist of set of trusted sensor nodes $i, j, k, \dots, n \in V$ and $(i, j) \in E$. For each $N(i, j) \in E$, it is assumed that node i is the sender node and node j is the receiver node. It is assumed that a faulty node k may drop packets randomly due to significant congestion and its behavior is modeled as shows in Eq.(1), while the malicious node always drops all the received packets.

$$F(k) = \begin{cases} 1 & k\ forwards\ the\ packets \\ 0 & k\ drops\ the\ packets \end{cases} \tag{1}$$

The proposed trust base routing scheme, TBSRP, extends routing mechanism of AODV protocol. The *Trust Evaluator, Trust database, Route Resolve* and *Route Setup* constitutes the four building blocks of proposed TBSRP scheme. The Trust Evaluator evaluates the trustworthiness of nodes. The trust database stores all necessary information required in trust establishment such as Node ID, packet forwarding ratio, direct and indirect trust values. The route setup is responsible for finding routes that contains all trusted nodes. If at some later time some malicious, faulty or energy deficient node becomes part of active route, route resolve process is initiated to inform source node to establish new trusted path.

2.1. Trust Evaluator

The trust evaluator evaluates the trustworthiness of neighbor nodes by overhearing their transmission in monitoring mode [24] and dynamically indentifies misbehaving nodes. The results obtained from monitoring packet forwarding behavior of nodes are stored in *Trust database*. Based on the packet forwarding behavior of node j, node i evalutes trust for node j represented by $T_{i,j}$ as in equation (2).

$$T_{i,j} = w_1 \times T_{i,j}Direct + w_2 \times T_{i,j}^{k}Indirect \quad (2)$$

$T_{i,j}Direct$ denotes the degree of direct trust node i has for node j, based on the node i's observation of packet forwarding behavior for node j. $T_{i,j}^{k}Indirect$ represents the average degree of indirect trust node i has gained using recommendations from its neighbors (k) for node j. The weight factors w_1 and w_2 are assigned to $T_{i,j}Direct$ and $T_{j,k}Indirect$ 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, $T_{i,j}Direct$ in equation (2), represents fundamental entity in constituting trust model and it is evaluated by monitoring the behavior of neighbor nodes. In order to estimate the direct trust, we compute packet forwarding ratio of a node. The packet forwarding ratio is the measure of number of correctly forwarded packets to the number of packets supposed to be forwarded, as shown in equation (3).

$$T_{i,j}Direct = {\sum_{p=0}^{N-1} Forwarded\ (p)} \Big/ {\sum_{p=0}^{N-1} Received\ (p)} \quad (3)$$

Every time a node receives a packet from neighboring node $Received\ (p)$ incremented by 1. Similarly, every time the node successfully forwards the received packets to intended destination $Forwarded(p)$ is incremented by 1.

An indirect trust in evaluated from the observations gained through interactions with neighbors who notify about their own direct observation for particular node. The indirect trust $T_{i,j}(t)$ is evaluated as:

$$T_{i,j}^{k}Indirect = \frac{1}{n} \sum_{k=1}^{n} T_{k,j} \quad (4)$$

$T_{k,j}$ represents the degree of indirect trust evaluated by node k (common neighbor of node i and node j). The evaluated indirect trust is exchanged as a part of recommendation with node i. $T_{k,j}$ is the average of existing trust evaluated by neighbors of node i (node k) for node j. Trust estimation involving indirect trust degree speeds-up the convergence of trust evaluating process. Based on packet forwarding ratio, trust model at node i expresses the behavior of neighbor j as either: *well-behave* or *malicious-behave*. If the packet forwarding ratio of node is above specified threshold γ, the node is considered as well-behave (trusted) node, otherwise it is considered as malicious node.

Figure 1 shows the analysis and efficacy of trust estimation mechanism of trust model. The weight factor plays an important role in trust estimation so we assigned higher weight to direct trust ($w_1 = 0.6$) than indirect trust ($w_2 = 0.4$) because it corresponds to direct observations gained by a node with its own interactions which are more accurate and timely available. It is observed that trust degree for well behave nodes increase linearly with time. Similarly, trust degree values for misbehaving nodes decreases as the simulation proceeds. It is due to fact that trust rating for well behaving nodes incremented each time as it cooperates in packet forwarding. On contrary, negative assessment for misbehaving nodes is increment as they drop the packets.

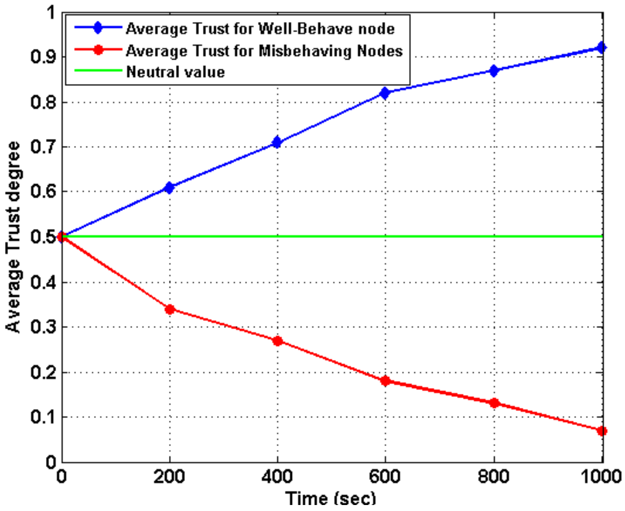
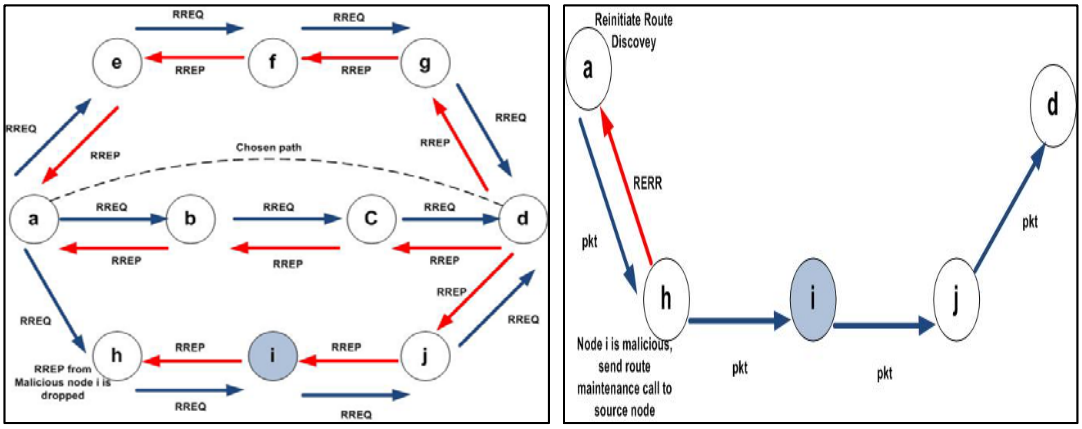


Figure 1. Average trust for misbehaving and trusted nodes

The design of our trust model does not make use of cryptography, thereby requiring least computations. In addition, our trust model avoids the use of resource intensive parameters for trust estimation such as security attributes, link quality and routing loop. Therefore, it offers light weight secure solution which neither imposes too many constraints nor requires any specialized set of resources. These features together with dynamic detection of misbehaving nodes makes our trust model an appropriate choice for resource constrained WSN as compared to existing schemes.

2.2. Route Setup

The *Route Setup* is responsible for establishing shortest and trusted route. The proposed scheme expands the route setup process of AODV in order to select reliable and efficient path that contains all reliable and trusted nodes. The distinguishing characteristics that leads to the selection of AODV protocol are: it is on-demand protocol means it enables to find routes when it is desired and reduces control packet overhead, provides fresh/latest routes information, capable of both broadcast and unicast routing, low connection setup time, more scalable and reduced storage cost. TBSRP make use of composite routing metric, where an equal and adaptive weights $\alpha = 0.5$ and $\beta = 0.5$ are assigned to node's trust level and hop count respectively which selects trusted and shortest paths for routing. High delivery ratio is achieved when reliable nodes are selected for delivery packets to destination. Consider a network shown in Figure 2(a) which assumes node a as the sender and node d as the receiver. Node a wishes to transmit data packets to node d, it broadcasts RREQ packet to its neighbors to initiate route discovery process. The neighboring nodes forwards RREQ packet to their neighbor nodes and also make reverse route entry for node a, same process continues till route request packet reaches to destination. Destination (node d) unicasts RREP packet to node a along the reverse route. If multiple RREQ packets have been received by destination from source via different routes, it sends multiple RREP packets along reverse routes to source node. This assists node a to make decision accordingly and appropriate path among available paths is selected comprising of only trusted nodes. When a RREP packet is received by an intermediate node h from its downstream neighbor i, which is not a destination node, node h refers to the trust table to check the trust value of node i. If node i is trusted one, it is included in the route, send RREP message to its upstream node(node a)and makes forward route entry for node d. RREP packet is dropped by node h if it find node i as unreliable node, and same process remains continue until route reply packet reaches at source node. Source node takes the routing path *a-b-c-d* as it is shortest path (contains all trusted nodes) and free of malicious nodes. The Figure 3 shows the flow chart for the route discovery of proposed TBSRP scheme.


RREQ
RREP
e
f
g
Chosen path
a
b
C
d
h
i
j
RREP from Malicious node i is dropped
Reinitiate Route Discovey
a
d
RERR
pkt
h
i
j
Node i is malicious, send route maintenance call to source node
pkt
pkt

(a) (b)

Figure 2. Route Discovery and Route maintenance process

2.3. Route Resolve

The responsibility of *Route Resolve* procedure is to send *RouteError* control packet to source node so that new route may be established when the condition $fr_{i,j} < \gamma$ becomes true meaning that an active route encounters some malicious or faulty nodes whose packet forwarding ratio is less than specified threshold value. In proposed scheme, route maintenance process is carried out whenever an intermediate node finds packet forwarding misbehavior caused by malicious or faulty nodes. A Route Error (RERR) message has been generated and forwarded to source node to find alternate route. Source node, reporting node and all intermediate nodes marks that route as an invalid route and source node starts new route discovery process. Consider the example shown in figure 2(b), where node h finds the condition $fr_{i,j} < \gamma$ has become true for node i, it consider the node i as misbehaving node and forwards RERR message to source node(node a) for finding a new reliable route.

3. Research Method

In this study, NS-2 simulator [25] has been used to analyze the performance of proposed TBSRP scheme. We consider blackhole attack for simulating misbehaving nodes where compromised nodes send fake route discovery packets to attract most of traffic. The behavior of faulty nodes is also simulated as some of the nodes drop packets randomly due to network faults or significant congestion level. Our simulation model is based on a network of 50 sensor nodes deployed randomly within an area of 1000m x 800m. The numbers of malicious and faulty nodes are varied from 0 to 5. In all experiments, the packet forwarding threshold (γ) is set to 0.6 while the trust threshold $(Trust_{thresh})$ is set to 0.8. All nodes are initialized with neutral trust value 0.5. We used IEEE 802.15.4 as the MAC layer protocol. Constant Bit Rate (CBR) traffic has been used for the flows with packet size equal to 1500 bytes while the simulation time is 1000 seconds. The performance TBSRP and AODV is analyzed in terms of packet delivery ratio, average end-to-end delay and normalized routing load.

4. Results and Discussion

Figure 4 shows the performance of TBSRP and AODV in terms of packet delivery ratio (PDR) against number of malicious and faulty nodes. It is evident from the results that both AODV and TBSRP shows increased PDR when there no malicious and faulty nodes in network.

The difference becomes prominent when at maximum number of malicious and faulty nodes as shown in Figure 4(a) and (b). The PDR for AODV decreases significantly by almost 90% as most of the traffic is attracted towards malicious nodes, as shown in Figure 4(a). By applying TBSRP, delivery ratio increases significantly as proposed scheme help the nodes to find trusted routes and isolate malicious nodes at earliest. Similarly, Figure 4(b) shows that TBSRP significantly improves the PDR when few faulty nodes drop random number of packets due congestion in active routes.

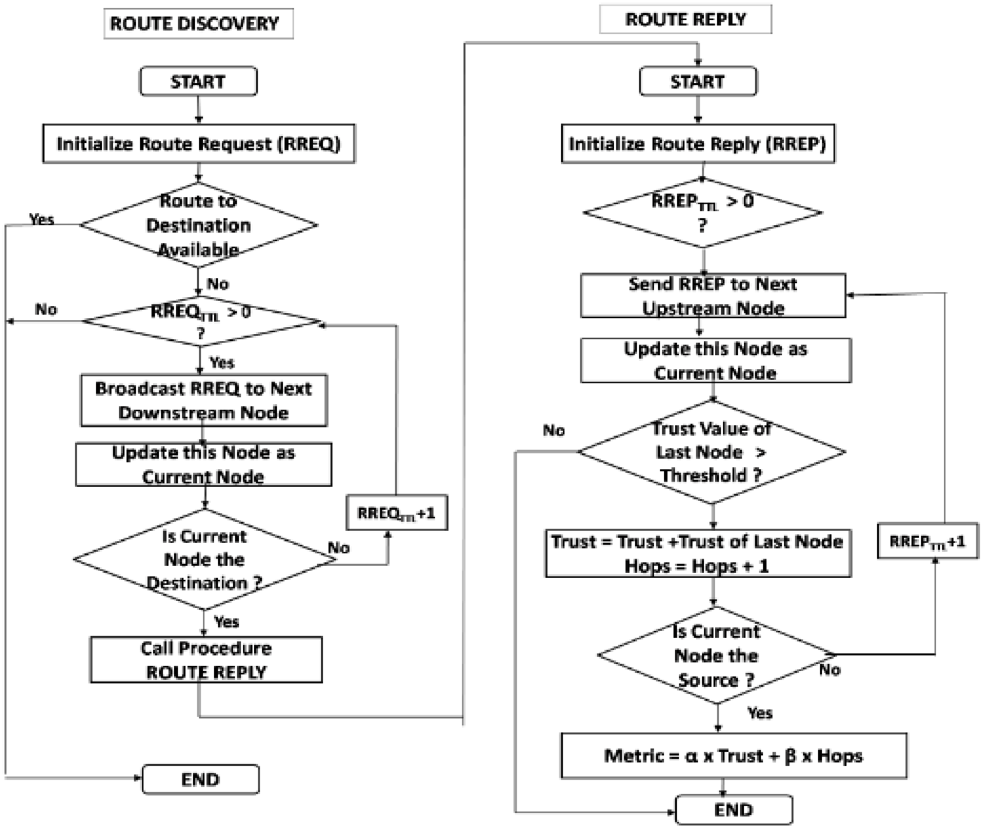

ROUTE DISCOVERY
START
Initialize Route Request (RREQ)
Route to Destination Available
Yes
No
RREQ$_{TTL}$ > 0 ?
No
Yes
Broadcast RREQ to Next Downstream Node
Update this Node as Current Node
RREQ$_{TTL}$+1
Is Current Node the Destination ?
No
Yes
Call Procedure ROUTE REPLY
END
ROUTE REPLY
START
Initialize Route Reply (RREP)
RREP$_{TTL}$ > 0 ?
Send RREP to Next Upstream Node
Update this Node as Current Node
No
Trust Value of Last Node > Threshold ?
Trust = Trust +Trust of Last Node
Hops = Hops + 1
RREP$_{TTL}$+1
Is Current Node the Source ?
No
Yes
Metric = α x Trust + β x Hops
END

Figure 3. TBSRP Route Discovery Flow chart

Figure 5 show the comparative results of average end-to-end delay for AODV and TBSRP under malicious and faulty nodes. When there are no misbehaving nodes in network, delay is similar for AODV and TBSRP. As the number of faulty and malicious nodes increases in the network, it creates more route disconnections which results in increased delay performance as shown in Figure 5(a) and (b). TBSRP relies on trusted and shortest routes avoiding misbehaving and faulty nodes therefore it shows better performance in term as average delay as compared to AODV where least number of packets delivered to destination in presence of increased number of malicious and faulty nodes.

The normalized routing load is an impotant design factor that should be considered while designing a routing protocols for WSN. As WSN is resource constrained network, increased routing load may badly effects the network lifetime of WSN. Figure 6(a) and (b) demonstrate the higher network overloads for AODV than TBSRP as it requires more number of retransmissions due to presence of malicious and faulty nodes in active routes. The more number of cotrol packets for route discvoeries further contributes to increased routing load of AODV. On contrary, the route remains more stable in TBSRP due to comprising of trusted nodes, therefore require less number of retranmissions and route discoveries.

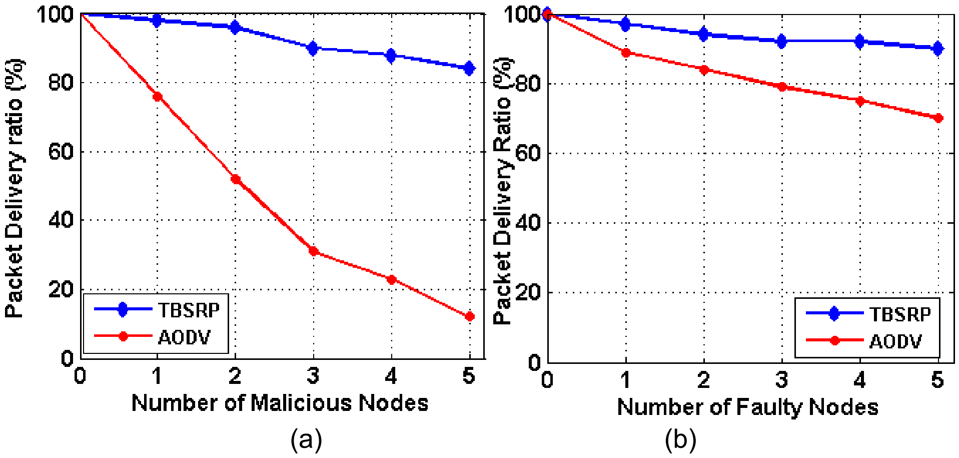


Figure 4. PDR performance with malicious and faulty nodes

To sum-up, the proposed TBSRP offers a multifacet routing strategy thereby minimizing the overall routing and network overheads for resource constrained sensor nodes. Table 1 presents the comparative analysis of proposed and existing schemes. TBSRP and TARF make use of composite routing metric which can adapt to dynamic nature of network. The proposed scheme incurs low routing and network loads as compared to existing schemes due to simple and robust design without involving too many broadcasts and exchange of control packets. Furthermore, proposed scheme can also detect faulty nodes responsible for dropping packets due to significnalt level of congestion.

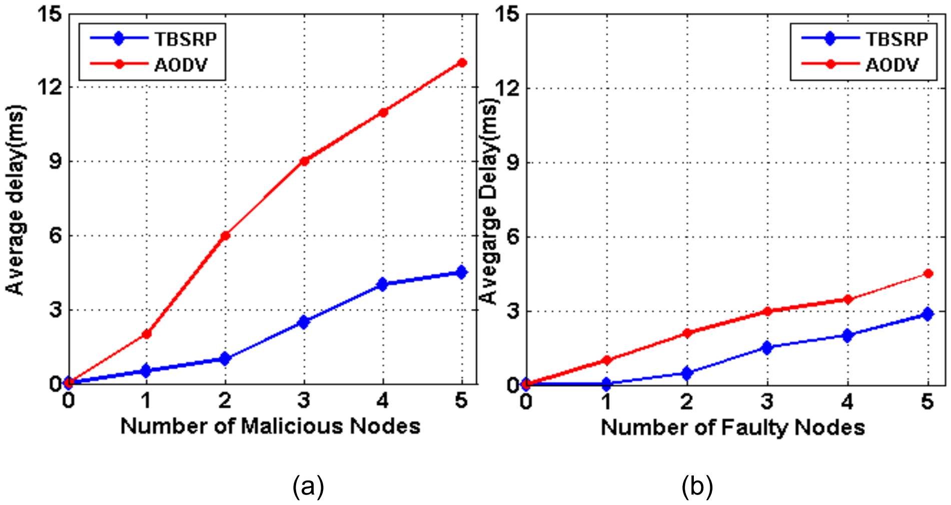
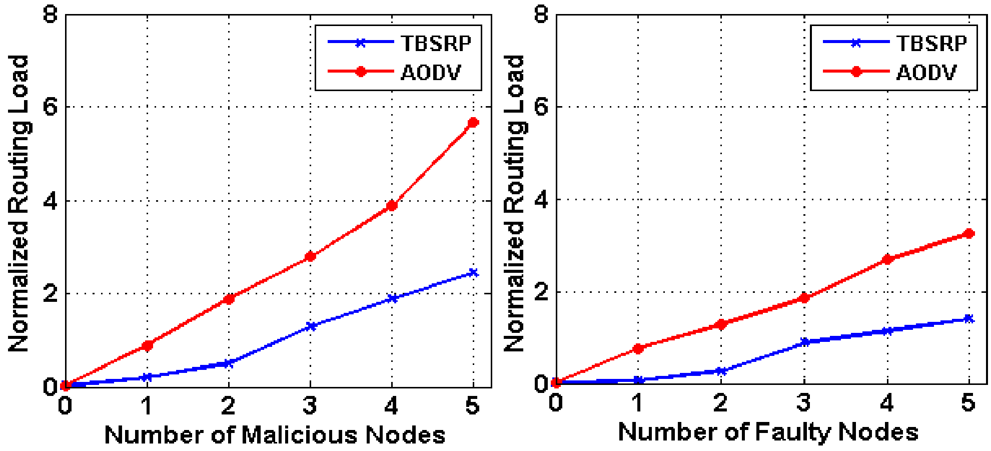


Figure 5. End-to-End delay performance with malicious and faulty nodes



(a) (b)

Figure 6. NRL performance with malicious and faulty nodes

Table 1. Comparative Analysis

	TBSRP	TARF	TARP	AODV
Routing metric	Composite	Composite	Singular	Singular
Routing overhead	Low	High	High	High
Network Load	Low	Medium	High	High
Fault Detection	Yes	No	No	No

5. Conclusion

In this paper, we proposed a lightweight and readily deployable Trust Based Secure Routing Protocol (TBSRP) for wireless sensor network to isolate malicious and faulty nodes. TBSRP can also re-route the packets to other routes if established route encounter packet forwarding misbehavior due to faulty or congested nodes. The simulation results prove the efficacy of proposed scheme. The performance of TBSRP is compared against AODV in terms of packet delivery ratio, average end-to-end delay and normalized routing load. The simulation results show that malicious nodes badly affect the overall performance of AODV and bring down the PDR and throughput to unacceptable ranges. TBSRP significantly improves the overall network performance and isolates malicious and faulty 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

[1] Akyildiz IF, Melodia T, Chowdhury KR. A survey on wireless multimedia sensor networks. *Computer Networks*. 2007; 51(4): 921–60.

[2] Putra EH, Hariyawan MY, Gunawan A. Wireless Sensor Network for Forest Fire Detection. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2013; 11(3): 563–74.

[3] Bangash JI, Abdullah AH, Anisi MH, Khan AW. A Survey of Routing Protocols in Wireless Body Sensor Networks. *Sensors*. 2014; 14(1): 1322–57.

[4] Mekki K, Zouinkhi A, Abdelkrim MN. Fault-tolerant and QoS based Network Layer for Security Management. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2013; 11(2): 363–72.

[5] Khan AW, Abdullah AH, Anisi MH, Bangash JI. A Comprehensive Study of Data Collection Schemes Using Mobile Sinks in Wireless Sensor Networks. *Sensors*. 2014; 14(2): 2510–48.

[6] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*. 2003; 1(2-3): 293–315.

[7] Zhou Z, Yow KC. Geographic Ad Hoc Routing Security: Attacks and Countermeasures. *Ad Hoc & Sensor Wireless Networks*. 2005; 1(3): 235–53.

[8] Kayarkar H. A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques. *International Journal of Advanced Networking & Applications*. 2012; 3(5): 1–14.

[9] Gupta C, Gupta K, Gupta V. *Security Threats in Sensor Network and their Possible Solutions*. IEEE International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA). 2012: 11–3.

[10] Haque MM, Pathan A-SK, Hong CS, Huh E-N. An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks. *KSII Transactions on Internet and Information Systems*. 2008; 2(5): 265–79.

[11] Hu Y-C, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*. 2003; 1(1): 175–92.

[12] Hu Y-C, Perrig A, Johnson DB. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*. 2005; 11(1-2): 21–38.

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

[14] Das ML. Two-factor user Authentication in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*. 2009; 8(3): 1086–90.

[15] Becher A, Benenson Z, Dornseif M. *Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks*. Technical Report. Springer Berlin Heidelberg. 2006.

[16] Cordasco J, Wetzel S. Cryptographic Versus Trust-based Methods for MANET Routing Security. *Electronic Notes in Theoretical Computer Science*. 2008; 197(2): 131–40.

[17] Chang K-D, Chen J-L. A Survey of Trust Management in WSNs, Internet of Things and Future Internet. *KSII Transactions on Internet and Information Systems*. 2012; 6(1): 5–23.

[18] Zhang C, Zhu X, Song Y, Fang Y. *A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks*. IEEE Proceedings on INFOCOM. 2010: 1–9.

[19] Zahariadis T, Trakadas P, Leligou HC, Maniatis S, Karkazis P. A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks. *Wireless Personal Communications*. 2012; 69(2): 805–26.

[20] Zhan G, Shi W, Deng J. Design and Implementation of TARF : A Trust-Aware Routing Framework for WSNs. *IEEE Transactions on Dependable and Secure Computing*. IEEE. 2012; 9(2): 184–97.

[21] Li X, Lyu MR, Liu J. *A Trust Model Based Routing Protocol for Secure Ad Hoc Networks*. IEEE Proceedings on Aerospace Conference. 2004: 1286–95.

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

[23] Eissa T, Abdul Razak S, Khokhar RH, Samian N. Trust-Based Routing Mechanism in MANET: Design and Implementation. *Mobile Networks and Applications*. 2013; 18(5): 666–77.

[24] Marti S, Giuli TJ, Lai K, Baker M. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*. Proceedings of the 6th ACM Annual international conference on Mobile computing and networking. New York. 2000: 255–65.

[25] Issariyakul T, Hossain E. *Introduction to Network Simulator NS2*. 2nd ed. Springer. 2012.