ISSN 2319 - 6629
Volume 3, No.4, June – July 2014
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/pdfs/2014/ijwcnt02342014.pdf


# TARF-Trust Aware Routing Framework for wireless networks

**Ms Veenaya Salve** ,M.E Student,**Prof. M.A.Bhalekar**, Assistant Professor,
MET BKC IOE ,University of Pune,Nashik, Maharashtra.

**ABSTRACT**
In multi hop routing, Wireless sensor Networks (WSNs) plays a vital role by preventing the routing information against the identity deception. The attacks such as sinkhole attack, wormhole attack, Sybil attack etc. are launched against the routing protocol which damages the network. Traditional cryptographic techniques or even trust aware routing protocols could not solve these severe problems. Thus to secure the WSN against such attacks, Trust aware Routing Frame work (TARF) is designed and implemented for dynamic WSN. TARF provide the trustworthiness and Energy efficient route without any known geographic information neither require tight time synchronization and proved to be effective against such attacks.

**Keywords :** TARF, Sensor Network, Routing, Wireless Sensor network (WSN)

## 1.INTRODUCTION

Wireless sensor network[1] contains battery powered sensor nodes having limited processing capabilities. Sensor nodes wirelessly send messages to a base station using narrow radio communication range through a multi-hop path. Wireless sensor networks [1] are used as an application in military surveillance and forest fire monitoring. But, in multi-hop routing an attacker may create traffic collision, drop messages, misdirect the communication channel and becomes the target of malicious attack [2]. Trust aware routing framework focuses on such kind of attacks in which misdirection of routing information is done. The attacks such as sinkhole attack, wormhole attack, Sybil attack [3] etc. are harmful and hard-to-detect and launched through identity deception against routing. Various routing protocols assume the honesty of nodes and focuses on energy efficiency [4], or allow the unauthorized participation by encrypting and authenticating packets.

Security as one of the most important goal in WSN becomes critical to achieve and also it is important to consider the energy use of battery and its robustness under any wild conditions. Even though the routing protocols provide the encryption and authentication for routing information, still a malicious node participate in the network using another valid node's identity, to overcome this drawback various routing protocols such as gossiping-based routing protocols provide certain protection against attackers by selecting random neighbors to forward packets, but becomes an overhead in propagation time and energy use.

Thus WSNs becomes more secure by providing TARF as a solution for routing information. The basic factor of TARF is to provide energy efficiency and cost worthiness for WSN. TARF can be implemented as a complete and independent protocol for routing information or it can be incorporated in existing routing protocol with least efforts producing a secure and efficient fully-functional protocol thus reducing the cost of an independent protocol. TARF secure WSN from various attacks exploiting the routing information, which is not achieved by other routing protocols. TARF do not require any known geographic information neither require tight time synchronization and proved to be effective against such attacks. Thus it results into improvement in the network performance even under the harmful attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks, and hostile mobile network condition. TARF is implemented as a ready-to-use module with low overhead and easy to use in existing routing protocols.

### *1.1 Routing Protocols in WSNs*

This section introduces the survey of routing protocols for WSNs [4]. Routing in WSNs can be classified as network structure and protocol operation protocol. Protocol is further classified as flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure .

**Flat-based routing-** All nodes in a routing path have equal roles or functionality.

**Hierarchical-based routing-** Each nodes in a routing path have different roles in the network.

**Location-based routing-** Sensor nodes positions are exploited to route data in the network. The protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation.

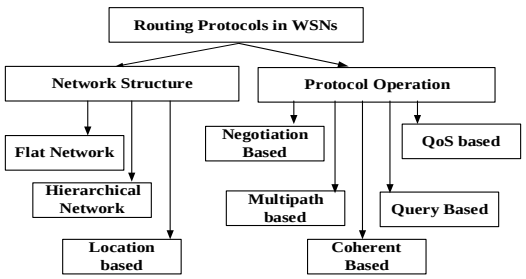


Figure 1: Routing protocols in WSNs: A taxonomy

The classification according to the network structure and protocol operation (routing criteria) can be as shown in Figure 1.

### 1.2 *Routing Challenges and Design Issues in WSNs*

**Wormhole attack:**
In this type of attack, the malicious node forges the identity of the nodes and use identity to participate in the network route, disrupting the network traffic. The routing packets, with their original header are replayed without any modification. When the packet in the routing network is send far away from the original node is called as Wormhole attack [3]. Thus in WSN, the destination node completely depends on the received packet to know about the sender's identity as a valid node. After stealing the valid identity the malicious node can easily misdirect the traffic which can be dropping the packets , forward packets to another node which is not supposed to be in routing path, or may form a transmission loop where the packets has to infinitely travel through the malicious node. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques.

**Sinkhole attacks:**
These attacks are another kind of attacks that can be launched after stealing a valid identity.

**Sinkhole attack:**
In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole".

**Sybil attack:**
In this attack, an attacker may present its multiple identities to the network while replaying the routing information. It performs same as sinkhole attack thus through replaying the routing information of multiple legitimate nodes; an attacker may present multiple identities to the network. A valid node can also launch all these attacks. The harm of such malicious attacks based on the technique of replaying routing information
is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though mobility is introduced into WSNs for efficient data collection and various applications it greatly increases the chance of interaction between the honest nodes and the attackers. Additionally, a poor network connection causes much difficulty in distinguishing between an attacker and an honest node with transient failure. Without proper protection, WSNs with existing routing protocols can be completely devastated under certain circumstances. In an emergent sensing application through WSNs, saving the network from being devastated becomes crucial to the success of the application.

## 2.LITERATURE SURVEY

In WSN, it is important to consider efficient energy usage for battery powered sensor nodes under any topological changes or wild conditions. Even after providing the strong encryption and authentication, the malicious node still participate in the routing network as an attacker which disrupt the network traffic, drop the packets. Security becomes an important factor for providing the secure routing.
Thus, trust management has been introduced into peer-to-peer network and general ad-hoc networks to improve the security and promote the resource sharing. Basically, trust manager assigns each node a trust value according to the previous performance which was beneficial to peer-to-peer networks and ad-hoc networks, but not resource-constraint WSN's. They could not address the attacks in the routing network. To overcome these limitations a reputation based approach was introduced to detect the un co-operative nodes in WSN. To fight against the "identity theft" threat arising from packet replaying information, trust management introduce TARF-Trust aware routing framework for wireless sensor networks. TARF identifies to misdirect those malicious nodes that misuse "stolen" identifies to misdirect packets by their low trustworthiness. TARF introduces the trust manager and Energy watcher as its components. TARF maintains the table for trust level values and energy cost values for known neighbors.

### 2.1 *Energy Watcher*

They are responsible for recording the energy cost for each known neighbor, based on different observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors.

### 2.2 *Trust Manager*

They are responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about undelivered data packets. Once N is able to decide its next-hop neighbor according to its neighborhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station.

## 3.IMPLEMENTATION DETAILS

The System flow model for TARF is implemented as follows.

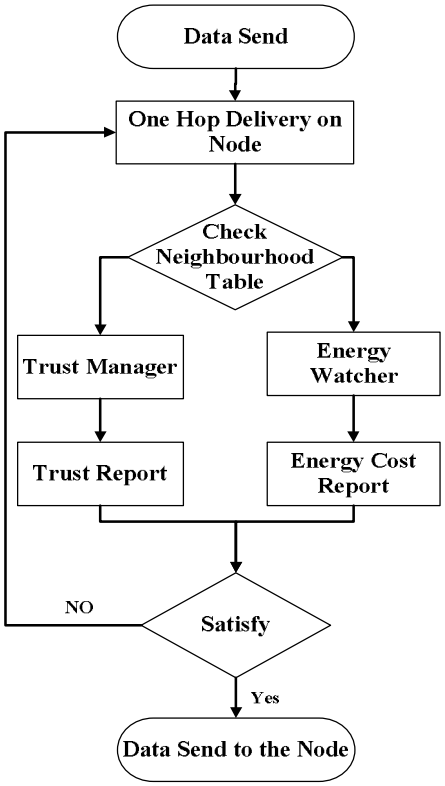


Figure 2: System Flow Diagram

From figure 2, it is observed that data packets are send on the router using one-hop delivery, the packets are send on the routing network where the trust values and energy cost report is considered generated by trust manager and energy watcher. After the complete analysis the packets are sending to the neighbor. For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is send to that next-hop node, it is totally unaware of what routing decision its next-hop node makes. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors.

### 3.1 System Architecture

In TARF, the messages are broadcasted from the base station to the destination node by sending the messages to all nodes over a network or by sending the messages to the specific nodes. TARF send this message along with Trust values and energy cost report to each nodes without any acknowledgement. These broadcast messages are sending over the whole network using the routing protocols. The freshness of a broadcast message is checked through its field of source sequence number. In other way, the messages are send with the energy cost report to only its neighbor once. When the nodes receive a message along with the energy cost report is not forwarded. Thus, to maintain such a neighborhood table in WSN with trust level values and energy cost values for certain known neighbors, two components Energy watcher and Trust manager is used which run on the node.

The system using TARF can be implemented as shown in figure 3.

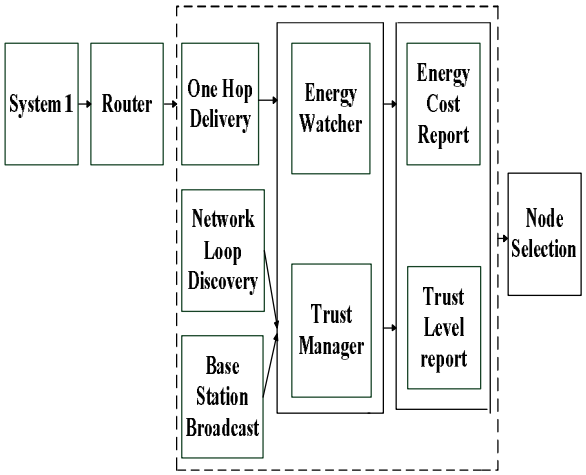


Figure 3: Block Diagram

**Energy Watcher:**

Energy watcher is responsible for recording the energy cost for each known neighbor, based on N's observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors. A compromised node may falsely report an extremely low energy cost to lure its neighbors into selecting this compromised node as their next-hop node; however, these TARF-enabled neighbors eventually abandon that compromised next hop node based on its low trustworthiness as tracked by Trust Manager.

Energy watcher computes the energy cost $E_{NB}$ for its neighborhood table and its own Energy cost $E_N$ for B as a next hop node. $E_{NB}$ denotes is the average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next-hop node being responsible for the remaining route. The re-transmission occurs until the acknowledgement is received or the specified threshold values are reached. The costs of one-hop transmissions are computed in $E_{NB.}$ Suppose instead of node B, N decides to take A as its next hop node after comparison of energy cost and trust level then the energy cost $E_{NA}$ is computed for the transmission. The straight forward relation can be established as:

$$E_{Nb} = E_{N \to b} + E_b \quad (1)$$

Since each known neighbor b of N is supposed to broadcast its own energy cost $E_b$ to N, to compute $E_{Nb}$, N still needs to know the value $E_{N \to b}$, i.e., the average energy cost of successfully delivering a data packet from N to its neighbor b with one hop. For that, assuming that the endings (being acknowledged or not)

of one hop transmissions from N to b are independent with the same probability $p_{succ}$ of being acknowledged, the average number of one-hop sending's needed before the acknowledgement is computed as follows:

$$\sum_{i=1}^{\infty} i.p_{succ}.(1-p_{succ})^{i-1} = \frac{1}{p_{succ}} \quad (2)$$

$E_{unit}$ is the energy cost for node N to send a unit-sized data packet once regardless of whether it is received or not. Then for unit sized data packet it can be given as

$$E_{Nb} = \frac{E_{unit}}{P_{succ}} + E_b \quad (3)$$

To compute $p_{succ}$, instead of using averaging method top compute after each transmission from N to B, N's energy watcher will update $p_{succ}$ based on whether the transmission is acknowledged or not with a weighted averaging technique. For representing the acknowledgement, if the ack is received then it given by 1 or 0. To obtain the value for $p_{new\_succ,}$ the average value of Ack and $p_{old\_succ}$ is averaged. psucc values are updated using two different weights $w_{degrade}$ and $w_{upgrade}$

$$p_{new\_succ} = \begin{cases} (1-w_{\text{degrade}}) \times p_{old\_succ} + w_{\text{degrade}} \times Ack, \\ \text{if } Ack = 0. \\ (1-w_{\text{upgrade}}) \times p_{old\_succ} + w_{\text{upgrade}} \times Ack, \\ \text{if } Ack = 1. \end{cases} \quad (4)$$

The two parameters wdegrade and wupgrade allow flexible application requirements.

**Trust Manager:**

Trust Manager is responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about data delivery. Once N is able to decide its next hop neighbor according to its neighborhood table, it sends out its energy report message: it broadcasts to all its neighbors its energy cost to deliver a packet from the node to the base station. The energy cost is computed by Energy Watcher. Such an energy cost report also serves as the input of its receivers Energy Watcher. At the beginning, each neighbor is given a neutral trust level 0.5. After any of those events occurs, the relevant neighbors' trust levels are updated. To detect loops, the Trust Manager on N reuses the table of smaller node id of a source node, a forwarded sequence interval [a, b] with a significant greater length in last period. If N finds that a received data packet is already in that record table, not only will the packet be discarded, but the Trust Manager on N also degrades its next-hop node's trust level. If that next-hop node is b, then $T_{old\ Nb}$ is the latest trust level value of b. if the loop is discovered then it is represented by 0 or else 1. As in the update of energy cost, the new trust level of b is

$$Tnew\_Nb = \begin{cases} (1-w_{\text{degrade}}) \times T_{old\_\text{Nb}} + w_{\text{degrade}} \times Loop, \\ \text{if Loop} = 0. \\ (1-w_{\text{upgrade}}) \times Told\_Nb + w_{\text{upgrade}} \times Loop, \\ \text{if Loop} = 1. \end{cases} \quad (5)$$

To detect the traffic misdirection by nodes exploiting the replay of routing information, *Trust Manager* on N compares N's stored table of smaller node id of a source node, forwarded sequence interval [a, b] with a significant greater length recorded in last period with the broadcast messages from the base station about data delivery. It computes the ratio of the number of successfully delivered packets which are forwarded by this node to the number of those forwarded data packets, denoted as Delivery Ratio. Then N's Trust Manager updates its next-hop node b's trust level as follows:

$$Tnew\_Nb = \begin{cases} (1-w_{\text{degrade}}) \times T_{old\_\text{Nb}} + w_{\text{degrade}} \times DeliveryRatio, \\ \text{if } DeliveryRatio < Told\_Nb. \\ (1-w_{\text{upgrade}}) \times Told\_Nb + w_{\text{upgrade}} \times DeliveryRatio, \\ \text{if } DeliveryRatio >= Told\_Nb. \end{cases} \quad (6)$$

## 4. RESULT ANALYSIS

TARF is implemented as an independent protocol or can be incorporated into existing protocol. Communication between different nodes is done using multihop routing techniques; using the shortest path algorithms the shortest path could be established to send the data packets over the network. The packets are sending along with energy cost and trust report generated by Energy watcher and trust manager. Depending on which the neighbor node is selected to further transmission and the selected neighbor node will be responsible for the further transmission. TARF enabled protocol detects the trusted node and avoid the packets from the DOS attacks which was hard-to-detect using another routing protocols. The existing TARF system is implemented for ideal conditions. It is implemented to work on unstable conditions which can increase the system performance. Figure 4 shows the performance analysis of the proposed and implemented TARF system.

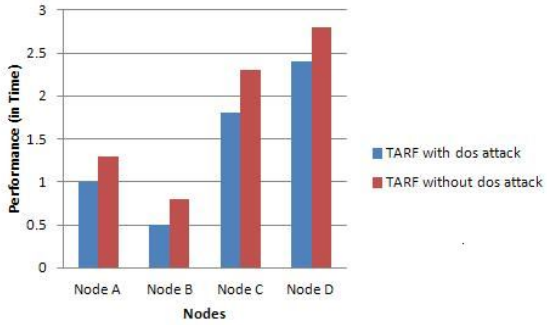


Figure 4:Result Analysis

Thus it is found that the DoS attack can be detected by this system which increases the system performance.

## 5.FUTURE CONTRIBUTION

It is generally hard to protect WSNs from wormhole attacks, sinkhole attacks and Sybil attacks based on identity deception. The countermeasures often requires either tight time synchronization or known geographic information [4]. FBSR, as a feedback-based secure routing protocol for WSNs , uses a statistics-based detection on a base station to discover potentially compromised nodes. But the claim that FBSR is resilient against wormhole and Sybil attacks is never evaluated or examined; the Keyed-OWHC-based authentication used by FBSR also causes considerable overhead. There also exists other work on trust-aware secure routing that is evaluated only through computer simulation. TARF enabled node currently works for an ideal conditions but it can also be developed for un-ideal conditions.

## 6.CONCLUSION

By using TARF (Trust aware routing framework), secure multi-hop routing in WSNs is done against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. Also using TARF, it effectively protects WSNs from severe attacks through replaying routing information and neither require tight time synchronization nor known geographic information. The resilience and scalability of TARF is proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves both static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks. TARF is ready-to-use module which can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols.

## ACKNOWLEDGMENT

I am very thankful to all the authors of papers which I have referred during my project work. I am also thankful to MET BKC IOE for providing all the requirements at each stage.

## REFERENCES

[1] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng "Design and Implementation of TARF: A trust-Aware Routing Framework for WSNs," IEEE 2012 Transactions on Dependable and Secure Computing, Vol. 9, Issue: 2, 2012

[2] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10), 2010.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and counter measures," in Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[4] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," Wireless Communications, Vol. 11, No. 6, pp. 6–28, Dec. 2004.

[5] A. Wood and J. Stankovic, "Denial of service in sensor networks," Computer, Vol. 35, no. 10, pp. 54–62, Oct 2002.

[6] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09). New York, NY, USA: ACM, pp. 1–14, 2009.

[7] "Performance analysis of mobile agent-based wireless sensor network," in Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), pp. 16 –19, 2009.

[8] W. Xue, J. Aiguo, and W. Sheng, "Mobile agent based moving target methods in wireless sensor networks," in IEEE International Symposium on Communications and Information Technology (ISCIT 2005), Vol. 1, pp. 22 – 26, 2005.

[9] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in Proceeding of the 7th Nordic Workshop on Secure IT Systems, 2003.

**Veenaya Salve** is post graduate student of computer engineering at MET Bhujbal Knowledge City, Nasik under University of Pune. Her areas of interest include network security ,wireless communication and data mining.

**Prof. Bhalekar Madhuri A. B.E., M.E. (Computer Sci & Engg)** Presently working at MET's BKC IOE, Nashik, Maharashtra, India as Assistant Professor in Computer Department. She has published and presented papers at National & International conferences on aspects of computer engineering. Her area of interest is Image processing, Automata, System Programming.