Secure Routing Protocol for WSN based on Trust Evaluation

Kokula Krishna Hari K, S. Prithiv Rajan

COO, BuyTheBook

Global President, Techno Forum Group

Abstract— A wireless sensor network is generally a vast network with large number of sensors nodes. It suffers from several constraints, like low computation capability, less storage capability, restricted energy resources, liability to physical capture, and therefore the use of insecure wireless communication channels. As the size and the density increases over the network, there are more chances of penetration of security in such network. These constraints build "security" in WSNs a challenge. Most of the protocols designed for wireless sensor networks consider energy efficiency but not security as a goal. In this present work, a Trust Based Secure Routing Protocol; TBSRP is designed to provide the security over the network. The presented work is a hybrid approach that performs the reliable node identification and provides the communication over the safe node. The presented work is divided in three main layers. In the first layer, the protocol level change is performed over the network. In the second layer, we have defined an authentication mechanism where Diffie – Hellman key exchange method is used to generate private and shared keys for every node in the network. At the third level of this presented work, a reliable routing approach is suggested. The trust analysis is performed here based on the honesty, reliability and the effective parameters. To demonstrate the utility of our trust based secure routing protocol, we apply it to a network having black hole attack. For each node, we identify the best trust composition and formation to maximize application performance. The presented TBSRP approach is basically an effective and reliable communication approach that can take the decision on next hop selection under the trust sector. Only a trustful node is eligible to transmit data over the network. TBSRP is compared with AODV routing protocol and the results of our work has shown that PDF is higher using TBSRP than that of AODV routing protocol.

Keywords — Trust management; Security in wireless sensor networks; Secure Routing in WSN.

I. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. There are some crucial aspects we always need to keep in mind when employed with these networks; security is one of them. We absolutely can't depend on any of our objects to be tamper-proof or use any kind of "trusted" computing platform since these characteristics often make the individual nodes prohibitively expensive. Security stipulation often vary with application and framework, but in general, security for wireless sensor networks should focus on the protection of the data itself and the network connections among the nodes. Some of the valuable data security requirements are confidentiality, integrity and authentication. When taking the network into consideration, we need to protect fair access to communications channels and we often need to obscure the physical location of our nodes. We must protect against malicious resource consumption, denial of service attacks, node capturing and node injection. Sometimes to guard the network from the effects of malicious nodes, secure routing is required by applications [1].

Because the communication among sensor nodes in a WSN is done by wireless transceivers, which tend to be extremely vulnerable to simple node attacks, shortcomings in a subsystem can easily be exploited to put on attacks on the whole network, even beyond the "sink." So it is very important to design sensor networks

with security in mind from their design stage, not as an additional feature of the system. Its main reason is that security always add some overhead, such as increased power requirements—something that's difficult to introduce in to an already-designed system. Firm coalition of security mechanisms in processing and communications simply allows for more efficient use of deficient resources.

The biggest dilemma for wireless sensor networks is that of network operational security. In other words, this problem involves a hierarchical alignment of nodes in networks and the secure communication between sensor nodes and base station. The security functions that we basically need, includes confidentiality, secure routing, detection of malicious nodes, and the ability to "repudiate" such nodes from the network.

In sensor networks each node is potentially a router for some other nodes. This formulates an entirely new set of susceptibilities in the network layer. For example, routers can become "neglectful," in that they selectively do not forward packets from other nodes, or they can become "selfish," in the sense that they choose to give preference to their own packets. Such behavior causes denial-of-service attacks.

Wireless sensor networks have much in common with wireless ad hoc networks, but many of the security mechanisms casted for ad hoc networks simply won't work for sensor networks. Unlike in ad hoc networks, every pair of nodes in a sensor network does not need to communicate. Additionally, in ad hoc networks many security mechanisms generally rely on public key cryptographic mechanisms, which may be too expensive in terms of resources as WSN is resource constraint. So, we could tryout to adapt a secure routing protocol based on secret-key cryptography, but it would place a heavy packet overhead in addition to necessitating the gathering of node state information.

Routing misdirection is an attack whereby malicious nodes advertise false routes to either inject fake traffic into the channel, direct traffic to a dishonest BS or node, exclude part of the network by exhausting its resources or avoid forwarding packets entirely. Such an attack can be countered using authentication, monitoring the network and redundancy techniques. Therefore security in Wireless Sensor Networks is of great importance to ensure the success of an application and secure data transmission. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations. The communication among sensor nodes is done by using wireless transceivers due to which they are vulnerable to security attacks. Sensor nodes may also be physically captured or destroyed by the adversaries.

The remaining of this paper is organized as follows. Some background overviews about subjective logic and trust based routing protocols are introduced in Section 2. Section 3, describes our proposed Trust Based Secure Routing Protocol for WSN, and its working algorithm. Simulation and Analysis is explained in section 4 where the performance and security analyses are presented in Section 5. Section 6 concludes the whole work.

II. Related Work

Working in resource-constrained environment, WSNs are prone to attacks by malicious and misbehaving nodes that try to compromise the routing protocol functionality. Most of the routing protocols projected for sensor networks don't seem to design to handle security related issues. Therefore there is a plenty of scope for attacks on them. Attacks on a WSN are primarily of two types: Active attacks use its energy to govern the routing information; whereas passive attack creates use of the knowledge from the system but does not have an effect on system resources. Some of the existing security solutions are cryptography, encryption and authentication. In our work, we have used Diffie -Hellman cryptographic protocol to establish a secret shared key ((g)ab mod p), over an insecure communication channel, between two parties that have no prior knowledge of each other. This key can then be used to encrypt consequent communications using a symmetric key cipher. It is extremely simple in its idea and it has a rather high level of cryptographic stability, which is based on the supposed complexity of the discrete problem of taking the logarithm [2, 3].

Neighbour based mostly communication without none trust worthiness creates a significant vulnerability in security related aspects of this network. In this type of situations, trust parameter plays an important role in all of the network activities. Continuous analysis of node's performance and their misbehavior (if any) about the node are used to calculate the trust value of this node with respect to other nodes. Using trust to improve security is an area of active research. Works like [4, 5, 6, 7, 8, 9, and 10] provide general frameworks for trust establishment and management in networks. A. Boukerch et. al. [4] proposes an agent-based trust and reputation management scheme (ATRM) for wireless sensor networks
which aims at managing trust and reputation locally with minimal overhead in terms of extra messages and time delay.

Xiaoqi Li et. al. [5] proposed a secure routing protocol TAODV which extends the basic functionality of AODV. It protects routing behavior in network layer for MANETS. Here, the nodes cooperate together to obtain an objective opinion about other node's trustworthiness. If a node communicates normally then its opinion from other nodes' point of view can increased and it is considered to be a trustworthy node of network. While a node performs some malicious behavior, it will be ultimately denied by whole network. The overheads incurred in computation are reduced without the needing certificates of request and verification at every routing operation.

Cuirong Wang et. al. [6] proposes a trust-based routing algorithm for ad hoc network tr-DSR. Security is the primary concern of the algorithm rather than optimality. In this paper, routing decisions are being made on the basis of trust parameters. A central trust authority is a superfluous requirement in this work. The routes discovered are not cryptographically secure but each one of them carries a confidence measure regarding its suitability called trust. The trust parameters are set in advance for all the nodes. The value of trust parameter ranges from -1 to +1, which represents a node from complete distrust to absolute trust. Two routes are maintained by each node to a destination, as will increase the number of different routes returned. Now the source has a better choice to select two maximal trust probability routes from the returned routes. The protocol then will use the path with the greatest trust value of route and less delay of packet. This leads to maximize the pre-emptive route creation by choosing the route that is expected to security.

Meka et al. [7] gives a trust-based framework for improving the security and robustness of ad-hoc network routing protocols. It uses 'Route Trust' as a metric for the source node to make route selection decisions. The security mechanism is based on incentives & penalties depending on the behavior of nodes. They permit source nodes to choose more trusted paths rather than just shorter paths during route discovery and help to isolate any malicious nodes from the network. Two trust values are associated with this protocol namely route trust and node trust. Route trust is calculated by each and every node for all the routes in its routing table; it is considered as a measure of loyalty or reliability with which a packet can reach the destination, if forwarded by the node on that particular route. Every node also maintains node trust on each of its neighbors. Node trust helps a node X to evaluate neighbor N's trust on a route passing through N. The route within the network is chosen on the basis of RSV- Route Selection Value. The source checks for all its available routes to the destination and it finally chooses the route which has the highest RSV.

Fenye Bao et al [8] proposed a trust management protocol for hierarchical routing which is highly scalable. This protocol deals with malicious and selfish nodes in the network. The authors have defined multiple parameters to identify the trust value. The trust components used by authors induces: intimacy, honesty, energy, unselfishness. A weighted value of these four components is being used to evaluate the overall reliability of a node. The trust evaluation is performed during the routing process in a peer-to-peer handshaking way. These works basically save the network from social network attacks.

In [9] a Redeemable Trust Based Secure Routing Protocol is proposed for WSN, where a special type of trust, predictability trust, is used to allow the speed of trust redemption to be controlled based on a node's previous behavior. If a node behaves as we have a tendency to expect it to behave, the redemption is fast. And if it behaves erratically, the redemption speed is slowed. As part of this trust mechanism, the authors

have used an idea of dynamic sliding windows to keep track of behaviours of each node. If a node has behaved badly recently, the sliding window is used to remember more bad behaviours for the computation of trust. If the node has behaved well most of the time, the scale of the window is smaller, and therefore less behavior is used to compute the trust value.

Guoxing Zhan et. al. gave a Trust Aware Routing Framework for wireless sensor networks (TARF) [10]. In this paper the author has defined an attack prevention approach by providing a trust worthy routing approach. While performing the communication over the node an identity proof is verified to save the network from harmful attacks. The authors have also defined the concept under energy effective approach. In TARF, an Energy Watcher and Trust Manager are used as its key components. The Energy Watcher keeps track of the energy consumed in one-hop transmission to its neighbors and it also maintains energy cost entries in its neighborhood table. Whereas the Trust Manager keeps track of loops formed in the network and it processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighborhood table. These two watchers track all the communication events and preserve the security and efficiency. TARF protects the network against wormhole and Sybil attacks.

Same kind of work performed by Anfeng Liu et al as done by Guoxing Zhan et al in designing TARF [10] respected to security and energy-efficiency. But this work is based on multipath routing as well as secret key sharing. The author has defined an energy consumption model based on distance and fading. The Security and Energy efficient Disjoint Route scheme (SEDR) [11] basically works as follows. First of all the packets are divided into shares by threshold- secret sharing algorithm. Then to increase the network security these packet shares are forwarded along the different routes distributed in the complete network.
The security analysis is performed for black hole attacks with different problem cases. The author has driven attack estimation respective to energy in case of single as well as multiple black hole attacks. The driven results from the approach shows the reliability of the network in terms of energy saving and security achieved.

In [14] TBAODV - Trust Based AODV is proposed. The performance of Ad-hoc On Demand Vector protocol is changed by including the source route aggregation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must help and trust each other in transmitting packets from one node to another. However, this constructive trust relationship can be exposed by malicious nodes. This exposure to malicious nodes may fabricate, modify or disrupt the orderly exchange of packets. Security needs all packets be authenticated before being used. This ensures authentication and helps increasing security. One problem is to provide efficient broadcast authentication which is must for MANET. Here, a routing algorithm is proposed which adds a field in request packet which stores trust value indicating node trust on neighbor. Based on level of trust factor, the routing information will be transmitted depending upon highest trust value among all. This not only saves the node's power by avoiding unnecessary transmitting control information but also in terms of bandwidth. Here, trusted path is used irrespective of shortest or longest path which can be used for communication in the network. Route trust value is calculated for the complete reply path which can be utilized by source node for next forthcoming communication in the network.

III. Proposed Work

This section emphasizes on a Trust Based Secure Routing Protocol (TBSRP) for wireless sensor network. In this present work, a trust based secure routing protocol is designed to provide security over the network. TBSRP is a hybrid approach that performs the reliable node identification and enables communication over the safe node. The presented work is divided in three main layers.

In the first layer, the protocol level change is performed over the network. According to this modification, a new trustworthy protocol is defined with trustworthy features and some trust parameters. To perform this, each node over the network is defined with one extra bit called trust. The trust analysis defined here is based on the neighbor node analysis. If the node is performing the communication with its neighboring

nodes effectively under different parameters, the node is called a trustworthy node. Such node can provide the reliable communication.

In the second layer, we have defined an authentication mechanism. To provide the authentication we have defined deffiehellman key exchange method. This approach is been used to verify the node validity at the time of handshaking. A node is called authenticated, if it proves its identity using the authentication approach being used. To perform the authenticated handshaking the encrypted information is transferred between the communicating nodes. Once the authentication satisfies, it can perform the authentication communication over the network.

At the third level of this presented work, a reliable routing approach is suggested. According to this approach, the next hop is identified based on the trust analysis. The trust analysis is here performed based on the honesty, reliability and the effective parameters. To perform such analysis, the neighbor node analysis is performed for the throughput, response time and the data loss basis. If a node is proven trustworthy in these parameters, the reliable and efficient communication will be performed over these nodes.

It ensures security on the basis of trust factor of each node in the network. The 'trust' factor of a node is calculated on the basis of misbehavior and errors encountered with neighbouring nodes. When data packets are subjected to transmit on a route, then sender will pass its data to a trusted neighbor node only. All the neighbouring nodes are checked for their trustworthiness based on their error rate and misbehaviour. Then the source node selects its most eligible neighbor to perform its further communication. This protocol is divided into two phases: authentication phase and trust phase.

1. Authentication Phase*:* First test is performed for the authentication of a node. A node encrypts its data with the shared secret key (g)ab which is calculated by two nodes previously; and transmits it the route. This key is known to only these two nodes who are actually communicating. At receiver's end the data will be decrypted by applying the inverse of (g)-ab. If a node replies back within a time period then it is assumed to be an authentic node. If its response time exceeds current time-request time; it will be considered as a compromised node. If it's a compromised node then find all the compromised node of i and the same process is repeated again for the remaining nodes to find the next authentic node of the network. This is the first level of trust.
2. Trust phase*:* At second level of trust, a node is checked for its trust vales. For this 3 conditions are being checked:
    1. If the response time of a node is less than the Intimacy Threshold AND
    2. Throughput of the node is greater than Honesty Threshold AND
    3. Energy of the node is greater than threshold energy.

If all these three conditions are satisfied, the current node will be considered as an eligible node for communication and it performs communication to next node in the network otherwise this node is considered to be a non-trust worthy node of the network. TBSRP is a protocol used for multipath routing also. It results in higher security in attack scenario. Ranging from the trust parameter, every neighbor is evaluated based on a set of trust metrics that include:

- Packet forwarding*:* To identify the nodes that judiciously transmit packets or decline to send packets, acting in an ungenerous manner, each time a source node sends a packet to a neighbor for further forwarding; it enters the promiscuous mode and overhears the wireless medium to see whether or not the packet was actually forwarded by the chosen neighbor.
- Authentication*:* The trust management module receives information from different blocks of applications associated with the trustworthiness of the neighbors. In case a node may choose between neighbors supporting different authentication mechanisms, the one with better security features should be preferred. Although this is often not an occurrence or behaviour facet monitored by the source node, it's listed here as an input to the trust analysis system.

- Remaining Energy*:* Even though the level of energy of each neighbour is not a real trust metric. In our proposed routing protocol, the remaining energy is used to indicate the node availability.

Algorithmic Steps for TBSRP:

Phase 1:

- Setup the network with N nodes and relative energy based parameters.
- Define Source S and Destination D for the network.
- Define the Trust Worthy Factors along with some specific threshold value called Intimacy Threshold, Honesty Threshold, Energy Threshold.
- Set Current_Node=Source
- Find the intermediate nodes over the path between S and D called P1,P2, …., Pm
- **For i=1 to m**
  Send Communication Request to Node(i) using Public Key.

  If

  (Accepted (Response) =Valid) Set Trust(Node(i))=1}

  End If

  Else

  Set Trust (Node(i)) = 0

  Find the compromising node of i and goto Step 8.

  End Else

Phase 2:

If

(Trust(Node(i))=1)

If

(ResponseTime(node(i)) < Intimacy Threshold And Throughput (Node(i)) > HonestyThreshold and Energy (node(i)) > EnergyThreshold)

Set TrustNode(i))=1

Set Node(i) as eligible node and perform the communication to next node

Set Current_Node= Node(i)

End If

Else

Set TrustNode (i)) =0

Print “Not Trustworthy Node”

End Else

End If

Find the neighbour nodes of node I called Ne1,Ne2...Nez

Find Most Eligible node from neighbour list in terms of energy and response time and replace node (i) by this node.

Node (i)= EligibleNeighborNode and go to step 8.

End For loop

IV. Simulation and Analysis

A. Simulation Model

To compare the proposed trust based secure routing protocol with AODV routing protocol and to check the effectiveness of the proposed method, a network scenario of 20 nodes has been taken for experiment. Area that we used for implementation of networks is 250m * 250m. Table 1 shows different simulation parameters and their associated values.

Table 1: Simulation parameters for the network establishment

Parameter Name	Value
Propagation type	TwoRayGround
No. of nodes	20, 30, 40, 50
Routing protocol	AODV
Simulation area (m x m)	250 x 250
Simulation time	Variable
Traffic type	CBR
Packet size	512 B
Initial energy	20 J
Tx, Rx power	0.5, 0.25 Mw

B. Performance Evaluation

We have used NS2 simulator to analyses and evaluate the performance of TBSRP. In our simulation study, we use one source-destination pair. The source node sends a Constant Bit Rate (CBR) flow of 50 data packets per second. Each data packet is 50 bytes in size. In order to evaluate the capability of AODV routing protocol on how it works in the presence of an attack in a WSN, we focused on these performance metrics as follows:

- Energy Consumption: Energy is one of the scarce resources for WSN. Energy consumption is the amount of energy drained by nodes in the network through communication and processing. So, the

total energy consumed, given as PE, can be calculated by adding all energy consumed by each nodes, n, for transmission (TX), received (RX) and processing throughout the simulation time.

- Packet Delivery Fraction: It is the fraction of the number of delivered data packet to the destination node. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol. PDF = Σ Number of packet received / Σ Number of packet sent * 100.
- Packet Latency: The time elapsed between the application layer passing a packet to the routing layer and that packet first being received at the destination.
- Percentage of Packet Loss: Packet Loss can be defined as the packets sent by the source and the packets dropped (loss) before receiving by the base station (sink). The percentage of packet loss, PL, is determined by calculating the ratio of packets unsuccessfully delivered to the sink, NL, to the total number of packets sent by mobile nodes, NS.

The packet delivery fraction for four networks with variable number of nodes in each for TBSRP and AODV are shown in Figure 1. From Figure 1, we observe that the packet delivery ratio for AODV is lower than that for TBSRP.

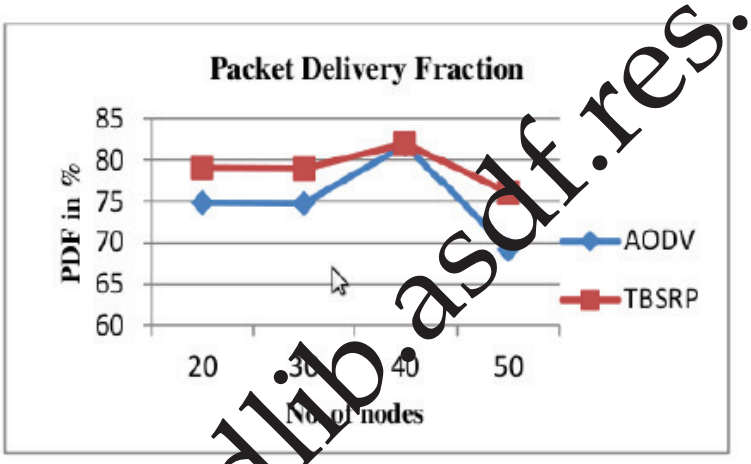

Fig 1: Comparison of Packet Delivery Fraction with TBSRP and AODV

Figure 2 shows the performance of a 20 nodes network with variable simulation time. The packet delivery fraction of TBSRP is improved with respect to AODV as the simulation.

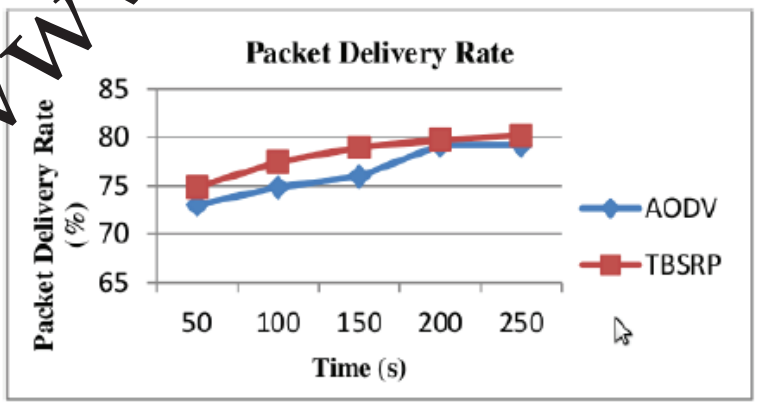

Fig 2: Packet Delivery Rate v/s Simulation time with TBSRP and AODV

Packet latency for TBSRP and AODV is shown in figure 3. For a network of 20 nodes, TBSRP has higher packet latency than AODV since AODV can build the route faster and therefore data can be sent faster.

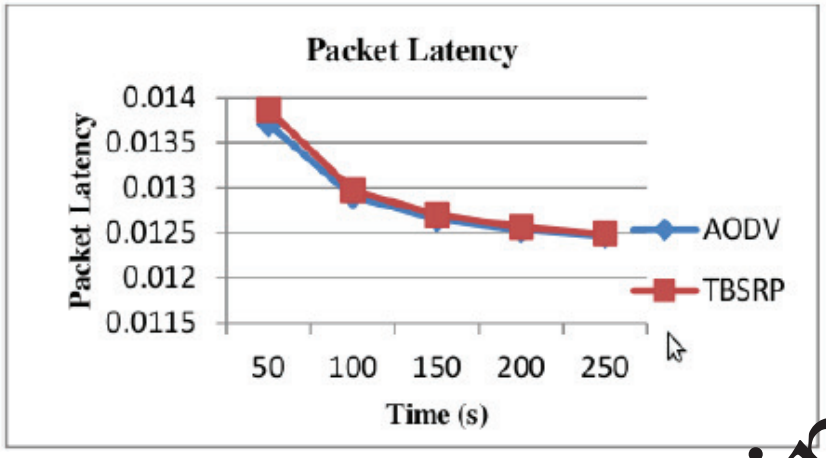

Fig 3: Packet Latency v/s Simulation time

TBSRP takes time in calculating trust parameters in the beginning. But as the trust parameters are calculated the packet transfer rate increases and packet delay decreases. Figure 4 shows the packet loss rate for a 20 nodes network with variable simulation time. The packet loss rate for both the protocols is almost same with a slight difference.

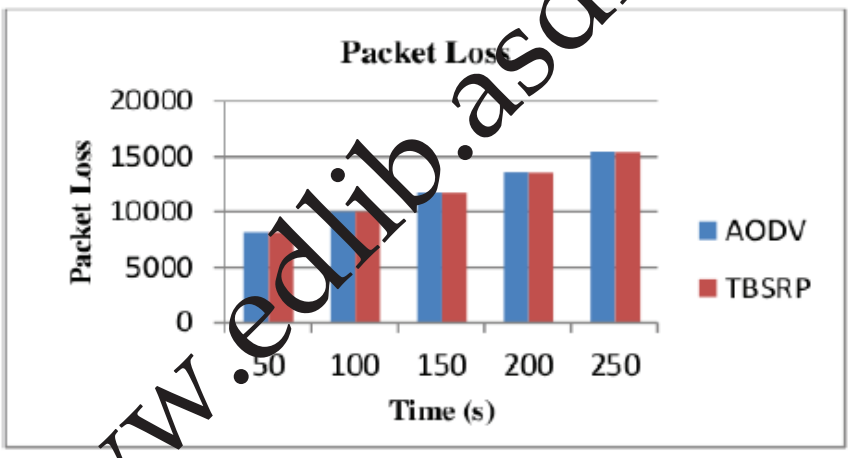

Fig 4: Packet Latency v/s Simulation time

This is because of the overhead involved in finding out the trustworthy nodes. Instead of the overhead the packet loss rate of TBSRP is near to that of AODV routing protocol.

V. Conclusion

Security is a significant issue in Wireless Sensor Networks. Insertion of malicious nodes may cause serious impairment to the security of a network. In this paper, we discussed about wireless sensor network and its vulnerability to attacks. Additionally it includes a review of some secure routing protocols associated with sensor networks. As most of the routing protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Most of the routing protocols used cryptographic techniques such as public key cryptosystem: RSA, Hashing etc. to secure the data transmission and the transmission link from different types of attacks. On the other hand, some routing protocols applied some way other than cryptographic techniques to achieve security like by choosing one of the paths from multiple paths to send data from sensor nodes to base station. The simulation work performed on NS2

simulator is described with graphs and network scenarios' screen shots. The performance is analysed in terms of throughput (no. of packets lost and transmitted) in the network. In our work, we have used Diffie – Hellman algorithm to generate private and shared keys at sender and receiver end. A Trust Based Secure Routing Protocol is proposed in which data is being routed through the trusted nodes present in the network. Moreover, the 'trust' factor of a node is calculated on the basis of 'misbehaviour and errors encountered with neighbouring nodes'. That means the trust factor will be calculated for every neighbouring node of the sender and then if the data packets will be transmitted via the most trustworthy neighbouring node. A comparison of our proposed routing protocol is done with AODV routing protocol showing higher throughput in terms of higher packet delivery ratio as compared to existing AODV. The presented approach is basically an effective and reliable communication approach that can take the decision on next hop selection under the trust vector. Only a trustful node is eligible to transmit data over the network.

References

1. Chris Karlof and David Wagner "Secure routing in wireless sensor networks: Attacks and countermeasures" Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, issue 2- 3, September 2003, pages 293-315.
2. en.wikipedia.org/wiki/Diffie–Hellman_problem
3. Kumar, V. "Secure-EEDR: Dynamic Key Exchange Protocol Based on Diffie-Hellman Algorithm with NOVSF Code-Hopping Technique for Wireless Sensor Networks" CCICC-ITOE 2010, pp 102-105.
4. A. Boukerch, L.Xu, and K.EL-Khatib " Trust-based security for wireless ad hoc and sensor networks" Volume 30, Issues 11-12, 10 September 2007, Pages 2413-2427. Computer Communications, 2007 – Elsevier.
5. Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" IEEEAC, 2004, vol. 2, pp. 1286-1295.
6. Cuirong Wang , Xiaozong Yang , and Yuan Gao, "A Routing Protocol Based on Trust for MANETs" H. Zhuge and G.C. Fox (Eds.): GCC 2005, LNCS 3795, Springer-Verlag Berlin Heidelberg 2005, pp. 959–964.
7. Kamal Deep Meka, Mohit Virendra, and Shambhu Upadhyaya "Trust Based Routing Decisions in Mobile Ad-hoc Networks".
8. Fenye Bao, Ing-Ray Chen, Moonjeong Chang and Jin-Hee Cho "Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-Based Routing" SAC'11, March 21-25, 2011, TaiChung, Taiwan. ACM 978-1-4503-0113-8/11/03 pp1732-1738.
9. "Redeemable Trust Based Secure Routing Protocol for Wireless Sensor Networks" http://dfcsc.uri.edu/research/trust.
10. Guoxing Zhan, Weisong Shi, and Julia Deng "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" IEEE Transactions on dependable and secure computing, Vol. 9, No. 2, March/April 2012. pp184-197.
11. Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen, and Xuemin (Sherman) Shen "Secure andEnergy-Efficient Disjoint Multipath Routing for WSNs" IEEE Transactions on Vehicular Technology, Vol. 61, No. 7, September 2012 pp3255-3265.
12. Introduction to PerlScript. http://www.cpan.org/authors/id/M/MS/MSERGEANT/PSIntro.html
13. Mangrulkar, R. S., and Dr. Mohammad Atique. 2010 Trust Based Secured Adhoc on Demand Distance Vecto Routing Protocol for Mobile Adhoc Network. In IEEE.
14. Theodore Zahariadis, Helen Leligou, Panagiotis Trakadas, Stamatis Voliotis, "Trust management in Wireless sensor Networks", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010, pp-52-68.
15. Theodore Zahariadis, Helen Leligou, Panagiotis Trakadas, Stamatis Voliotis, "Trust management in Wireless sensor Networks", European Transaction on Telecommunications, 2010.