Volume-3, Issue-8, August-2014 • ISSN No 2277 - 8160

Research Paper | Computer Science

Malicious Node Detection using Belief based Protected Routing (BPR) in Autonomous Wireless Sensor Network

Dr. M. Pushparani — Professor and Head, Dept. of Computer Science, Mother Teresa Womens' University, Kodaikkanal, India

Komathi A. — Research Scholar, Bharathiar University , Coimbatore, India, Assistant Professor , Department of Computer Science & Information Technology Nadar Saraswathi College of Arts and Science , Theni , India

ABSTRACT

Over the years, wireless sensor networks have been extensively used for monitoring applications. The data sensed by various devices in the network are being reported to the control station at frequent intervals. Secure routing becomes a crucial need as the applications become vital. To provide protected routing in autonomous wireless sensor networks is to also enhance routing performance in the network. In this work, a belief factor is proposed based on which each next hop is selected for routing from a source to a destination. This factor not only assists in route selection process but also helps in the identifying malicious nodes in the network. Performance evaluation and analysis is performed using the network simulator to exhibit the efficiency of the proposed work.

KEYWORDS : Autonomous wireless sensor network, belief factor, malicious node, quality of service, threshold

1. Introduction:

Wireless sensor networks have aided automation in application area monitoring in the recent years to a vast extent. The low-powered monitoring devices use their transceivers to sense information and report to a base station. The data transmitted by these low powered devices use the available routes to make it to the base station in the best available manner. Generally the wireless sensor network is used in the hostile environment with no human existence. So, each sensor node should be tolerant to failure and loss of link between the nodes. The need is the sensor node uses its intelligence to recover from the problem. The network which supports autonomous formation of connectivity and routing packets to destination is called as Autonomous wireless sensor network.

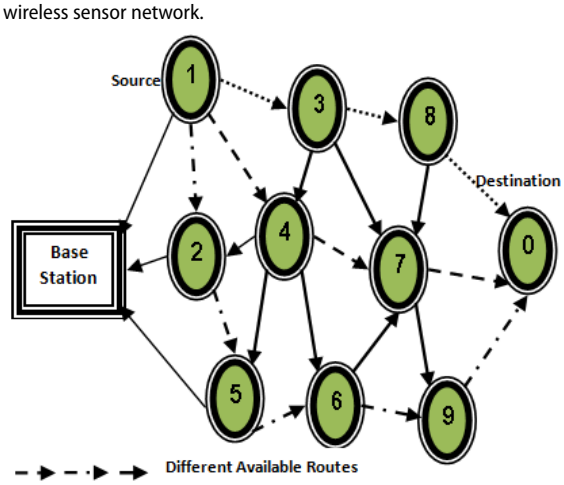

Figure 1: Example of an autonomous wireless sensor network

In autonomous wireless sensor network data gathered by the sensors is aggregated and stored locally, rather than being sent to a base station or sink for processing. To ensure that intermediate node selection is performed in a secure way, a node security provision algorithm is mandatory. Many solutions have aimed at providing secure route selection in wireless sensor networks; however, the need for security is always a demand, especially because of increased malicious activity in autonomous wireless sensor networks.

In this work, a Belief based protected routing mechanism is proposed simulated and portrayed that serves as a feasible solution in the maximum reduction and detection of malicious nodes in an autonomous wireless sensor network. The estimation of the belief factor is described in the sections that follow along with a simulation analysis discussion.

2. Problem Statement:

The autonomous wireless sensor network is mainly used in the critical application. So, we are in the need to provide safe path while transferring the data to the corresponding destinations. Secure routing is a difficult problem in wireless sensor network due to resource limitation. Thus belief based protected routing algorithm is reviewed to tackle the problems. One of the most popular existing solutions is the Biological inspired Secure Autonomous Routing Protocol (BIOSARP). The major disadvantage of this scheme is that it does not consider the quality of service while routing the data packets. But, the proposed routing scheme considers the quality of service and provides efficient routing in a secure manner. In autonomous wireless sensor network, there is no centralized control. So each and every node should maintain the belief value of its neighbor.

3. Existing Solutions

Existing works that aimed at providing solutions to this problem include clustering solutions. A decentralized clustering algorithm for wireless sensor networks based on the structure of social insect colonies was proposed in (Cheng, Tse & Lau, 2011). A cluster-based energy balancing method (Ai, Turgut & B¨ol¨oni, 2005) used hierarchical clustering to keep the network functioning for longer duration of time. But both (Ai et al., 2005) and (Cheng et al., 2011) do not consider the node behavior during communication. Hierarchical trust management (Aivaloglou, 2009) was then introduced to form a trust model based on network pre-deployment information on topology, capabilities of the nodes in terms of data flows across the network and the behavioral aspects of the nodes during communication. Although energy is also considered for the design model, efforts have not been taken to enhance the network lifetime. The works by (Cho, Swami, Chen, 2011), (Jamal, 2004) and (Lopez, Roman, Agudo, Fernandez-Gago, 2010) provide a survey on the trust management methods for wireless sensor networks whereas (Bao, 2012) extends the trust management technique to the intrusion detection mechanism as well. In all cases the either the quality of service and/or privacy provision or energy enhancement is addressed.

BIOlogical Inspired Secure Autonomous Routing Protocol (BIOSARP) is a suitable and efficient protocol that meets the enhanced WSN requirements by providing better delivery ratio and less energy consumption (Saleem, Fisal, Abdullah, Ariffin, 2010). However, the QoS behavior of the nodes is not considered while routing. To overcome

this disadvantage, we propose a solution and use BIOSARP as a standard of comparison to prove the efficiency of the proposed work.

4. Proposed Solution - Belief based Protected Routing (BPR):

In this scheme, we have to calculate the belief value of each and every sensor node present in the network by using the belief function. The belief value is getting change dynamically. The belief value is calculated by using the following formula:

$$BF=N_{honesty}+N_{energy}+N_{lossratio+}\ N_{QOS} \quad (2)$$

Each and every node's belief value is calculated by getting the above value from its entire neighbor. The ratio of the value collected from neighbor sensor is assigned as the belief value of the node. For the particular period of time, the setup server should update the belief value based on its neighbor's vote. After that, the belief routing algorithm is applied to route the data packets from source to destination.

4.1 Belief routing algorithm:

The belief based routing protocol uses the belief routing algorithm and authentication algorithm for the BPR process.

```
The source node sends RREQ to its neighbor
For all of its neighbor N_i {
        If authenticate (S, N_i) == true {
        Rebroadcast the RREQ to its neighbor
        Update the belief value
Until N_i= Destination
Else
                Update the belief value of N_i
                Mark N_i as distrusted node
    End If
```

To provide the authentication between the nodes we have to set the threshold value. The threshold value is compared with belief value to decide authentication.

```
Authenticate (S, N_i) {
    If BF (N_i) <TH_i {
                Return false
    Else
                Return true
    End if
```

4.2 Malicious Node Detection using BPR:

The node malicious detection mechanism is incorporated by modifying the authentication algorithm proposed in the BPR. If the belief factor (BF) of a particular node is k times lesser than the threshold then, the node is reported as a malicious node to its neighbors. The equation 2 shows how k is estimated.

$$k(Ni) = \frac{THi}{BF(Ni)} \quad (2)$$

The value is the factor by which the node N's BF value differs from the threshold TH at the instant i. If the value of is less than 0.25, then the neighbor that estimates the node N's BF marks it as a malicious node and also notifies the same to the common neighbors.

```
Authenticate (S, N_i) {
    If BF (N_i) <TH_i {
        Estimate k(N_i)
            If k(N_i) <0.25
                Mark N malicious
  Notify common neighbors
                End if
    Else
                Return true
    End if
```

The node detection mechanism along with the BPR is illustrated in the figure 2.

By using our proposed scheme, we are going to provide the security against selfish and malicious behavior of the sensor node present in the network. Our proposed scheme will provide better delivery ratio with less energy consumption.

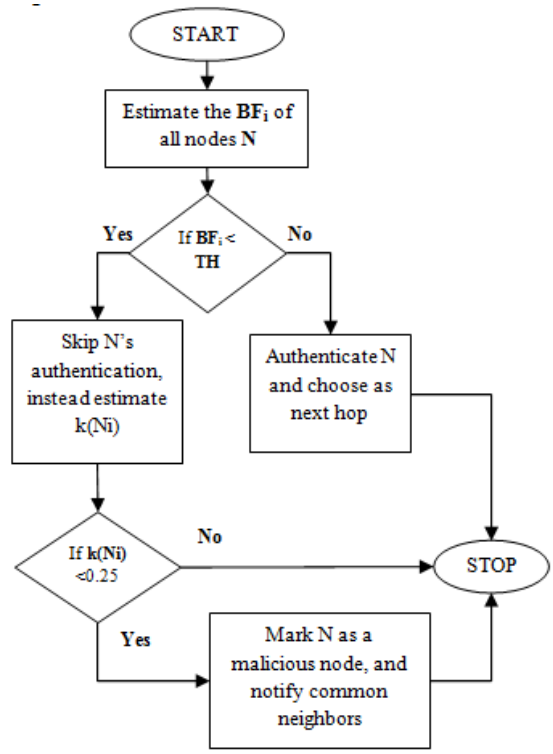

Figure 2: Working of the Malicious Node Detection using Belief based Protected Routing (BPR)

5. Simulation Analysis:

The simulation of the proposed Malicious Node Detection scheme using Belief based Protected Routing (BPR) is performed by using the simulator NS2. Network simulator is a discrete event time driven simulator. NS2 is open source software which uses C++ and Tool Command Language (TCL) for simulation. In the simulations performed the efficiency of the proposed system is exhibited by evaluation of the parameters: packet delivery ratio, delay ratio and energy consumption. The simulation parameters used in the simulation of the Malicious Node Detection scheme using BPR is tabulated below in Table 1.

Table 1: Simulation Parameters of BPR

Parameter	Value
Channel Type	Wireless Channel
Radio Propagation model	TwoRayGround
Network interface type	WirelessPhy
MAC Type	IEEE 802.11
Interface Queue Type	PriQueue
Link Layer Type	LL
Antenna Model	Omni Antenna
Simulation Time	100 ms
Number of Nodes	21

5.1 Packet Delivery Ratio:

The total number of packets successful delivered with respect to the number of packets sent can be obtained from the packet delivery ratio.

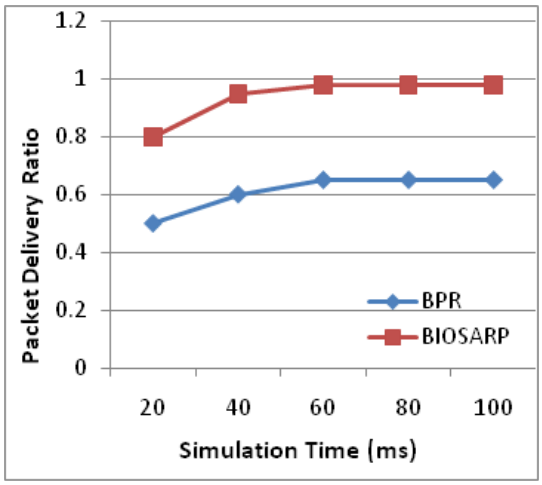

Figure 3: PDR of BPR and BIOSARP

Packet Delivery Ratio is denoted as PDR and estimated by equation (3).

$$PDR = \frac{Total\ pkts\ recieved}{Total\ pkts\ Sent} \quad (3)$$

The figure 3 shoes that the PDR is increased for that of BPR in comparison with BIOSARP over the simulation time.

5.2 Packet Loss Ratio:

The total number of packets lost during simulation of the BIOSARP and the BPR protocols is plotted in the figure below. The number of packets lost in the BPR simulation over the time is reduced when compared to that of the BIOSARP.

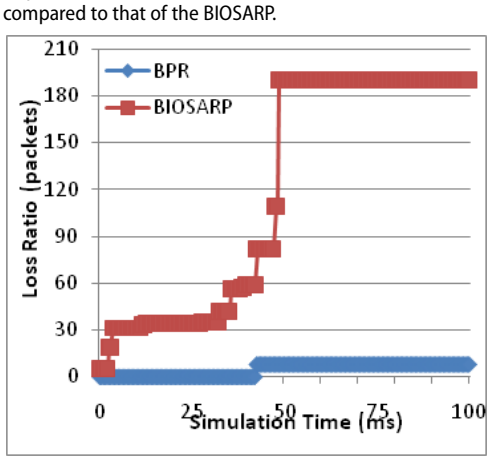

Figure 4: Packet Loss ratio of BPR and BIOSARP

5.3 Malicious Node Detection:

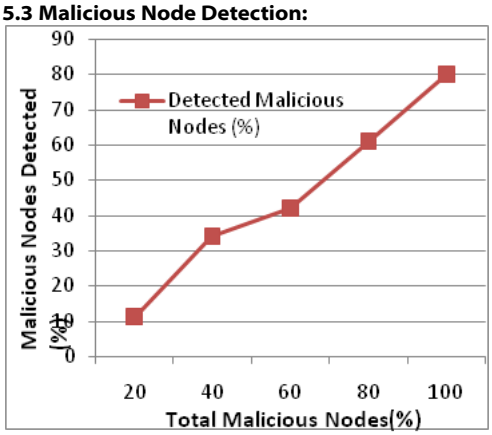

Figure 5: Malicious Nodes detected by BPR

The proposed scheme is first tested to see how many malicious nodes it is able to detect when a fixed number of malicious nodes were modeled in the network.

5.4 Packet Delay Ratio:

The total delay occurred in BPR is lesser during data transmission in the network as plotted in the figure 6.

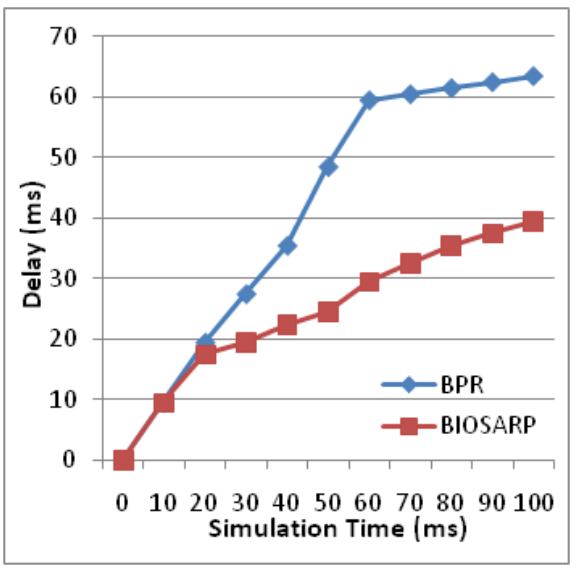

Figure 6: Packet Delay ratio of BPR and BIOSARP

5.5Residual Energy

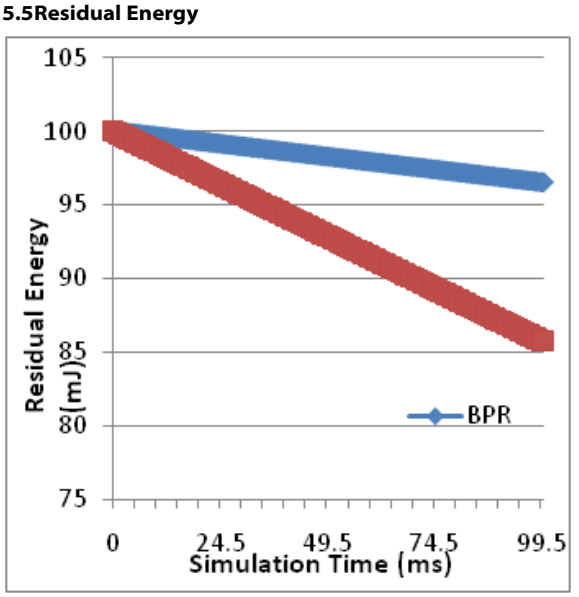

Figure 7: Residual Energy of BPR and BIOSARP

Residual energy plot helps in finding the energy efficiency of the network. The graph plotted in figure 7 shows that the residual energy of the BPR is higher than that of BIOSARP. The minimization of energy consumption is because while belief factor helps in finding an energy efficient next hop while finding the destination.

6. Conclusion

The belief based protecting routing protocol is used to find an efficient route using the behavioral aspects of a node that not only aid in the quality of service enhancement but also improves the network lifetime. Security and privacy are additional features provided by this protocol as a consequence of the malicious node detection process performed. Hence the BPR routing is energy efficient and secure.

Future works aim at providing reinforcement to the different attackers while also retaining the current efficiency in terms of quality of ser-

vice.

REFERENCES

Ai, J., Turgut, D, & B¨ol¨oni, L. (2005). A Cluster-based Energy Balancing Scheme in Heterogeneous Wireless Sensor Networks", In Proceedings of the 4th International Conference on Networking (ICN'05), pp. 467–474. doi: 10.1007/978-3-540-31956-6_55 | Aivaloglou, E., Gritzalis, S, (2009). Hybrid trust and reputation management for sensor networks, Wireless Networks, 14th Oct. doi: 10.1007/s11276-009-0216-8. | Bao F., Chen I.R., Chang M., and Cho J.H, (2012). Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, vol. 9, no. 2. doi: 10.1109/TCOMM.2012.031912.110179 | Cheng, C., Tse C.K, & Lau F.C.M, (2011). A Clustering Algorithm for Wireless Sensor Networks Based on Social Insect Colonies, IEEE Sensors Journal, Vol. 11, No. 3, March 2011, doi: 10.1109/JSEN.2010.2063021 | Cho J.H, Swami, A. & Chen I.R., "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Comm. Surveys and Tutorials, vol.13, no.2, pp. 562-583. doi: 10.1109/SURV.2011.092110.00088 | Jamal N. Al-Karaki Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", ICUBE initiative of Iowa State University, Ames, IA 50011(2004). doi:10.1.1.122.7063 | Lopez, J., Roman, R., Agudo, I., Fernandez-Gago, C., (2010). "Trust Management Systems for Wireless Sensor Networks: Best Practices", Computer Communications Volume 33, Issue 9, 1 June, pp. 1086–1093. doi: 10.1016/j.comcom.2010.02.006 | Saleem K., Fisal N., Abdullah, M.S & Ariffin S.H.S, (2009). Biological inspired secure autonomous routing mechanism for wireless sensor networks, Int. J. Intelligent Information and Database Systems. doi: 10.1109/ACIIDS.2009.75 |