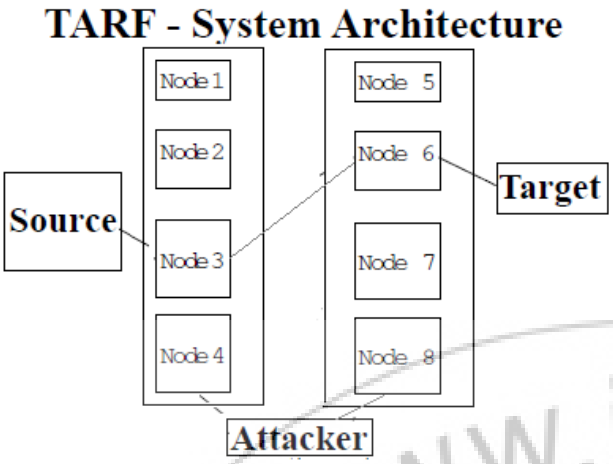
www.ijsr.net
IJSR
ISSN (Online): 2319-7064

www.ijsr.net
IJSR
ISSN (Online): 2319-7064



4. Formulas for selecting the next node from each level to send the data from source to Destination

1. **To calculate the trust percentage of each Node:**

For all **Nodes in Level1** do:
Trust_Percentage = Ack_received / Total_packet_sent

Forall**Nodes in Level2** do:
Trust_Percentage = Ack_received / Total_packet_sent

2. **To calculate Energy Percantage of each node:**

Forall**Nodes in Level1** do:
Energy_Percentage = 100 - Energy_Cost

Forall**Nodes in Level2** do:
Energy_Percentage = 100 - Energy_Cost

3. **To calculate Node Weight of each Node:**

Forall**Nodes in Level1** do:
Node_Weight = Trust_Percentage + Energy_Percentage

Forall**Nodes in Level2** do
Node_Weight = Trust_Percentage + Energy_Percentage

4. **Select the Node to transfer the data:**

Level1_Node = (Greatest_Node_Weight(Fromall **Nodes in Level1**)) && (Status = Active)

Level2_Node = (Greatest_Node_Weight(Fromall **Nodes in Level2**)) && (Status = Active)

Algorithm for TARP:
Step 1. Get all nodes in the Network.
Step 2. Group them into layers.
Step 3. Calculate the Node Weight of each node in all the Layers using formula.
For all **Nodes** in **Level1** do **Node Weight = Trust Percentage + Energy Percentage.**
Forall**Nodes** in **Level2** do
Node_Weight = Trust_Percentage + Energy_Percentage.
Step 3. Select one node from each as "next hop".
Level1_Node = (Greatest_Node_Weight(Fromall Nodes in Level1)) && (Status = Active)
Level2_Node = (Greatest_Node_Weight(Fromall Nodes in Level2)) && (Status = Active)
Step 4. Send the data from Source to Destination through Level1_Node and Level2_Node.

Snapshots

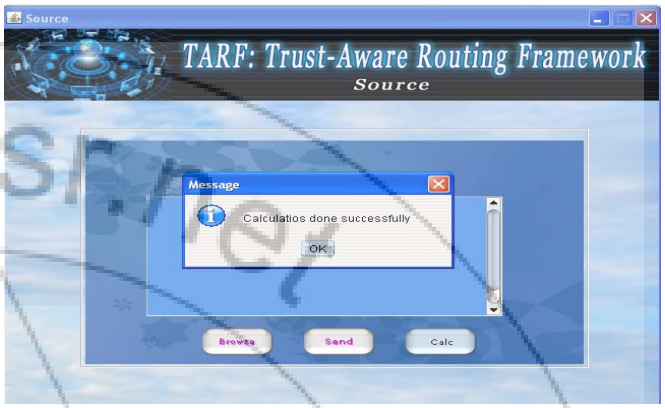


Figure : source node. When we click calc button trust and energy percent of all the nodes of level1 router will be calculated in the database.

Conclusion

We have designed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs 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.

Our main contributions are listed as follows. (1) Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.

Researcher'sfuture work is to further evaluate TARF withlarge-scale WSNs deployed in wild environments and to study how to choose parameters involved for specific applications. They believe that the idea of TARF can also be applied to general ad hoc networks and peer-to-peer networks to fight against similar attacks.

References

[1] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routingframework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the1st IEEE International Workshop on Sensor Network Protocols andApplications*, 2003.
[3] M. Jain and H. Kandwal, "A survey on complex wormhole attack in wireless ad hoc networks," in

Proceedings of International Conference on Advances in Computing, Control, and TelecommunicationTechnologies (ACT '09), 28-29 2009, pp. 555 –558.

[4] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *Proceedings of IEEE International Conference on Wireless and MobileComputing, Networking and Communications(WIMOB '08)*, 12-14-2008, pp. 526 – 531.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks:Analysis and defenses," in *Proc. of the 3rd International Conference on Information Processing in Sensor Networks(IPSN'04)*, Apr. 2004.

[6] J. Hee-Jin, N. Choon-Sung, J. Yi-Seok, and S. Dong-Ryeol, "A mobile agent based leach in wireless sensor networks," in *Proceedings of the 10th International Conference on Advanced CommunicationTechnology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[8] A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput.Commun.*, vol. 30, pp. 2826– 2841, October 2007.

[9] C. Intanagonwiwat, R. Govindan, D. Estrin, Directeddiffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of the ACM Mobi-Com'00, Boston, MA, 2000, pp. 56–67.

[10] C. Perkins, Ad Hoc Networks, Addison-Wesley, Reading, MA, 2000.

[11] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Nextcentury challenges: scalable coordination in sensor networks, ACM MobiCom'99, Washington, USA, 1999, pp. 263–270.

[12] N. Bulusu, D. Estrin, L. Girod, J. Heidemann, Scalablecoordination for wireless sensor networks: self-configuring localization systems, International Symposium on Communication Theory and Applications (ISCTA 2001), Ambleside, UK, July 2001.

[13] Al-Karaki, J., Kamal, A.: Routing techniques in wireless sensor networks: a survey. IEEEWireless Communications 11(6), 6–28 (2004).

[14] Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proceedings of 1996 IEEE Symposium on Security and Privacy, pp. 164–173 (1996)

[15] Boukerche, A., El-Khatib, K., Xu, L., Korba, L.: A novel solution for achieving anonymity in wireless ad hoc networks. In: Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, pp. 30–38 (2004)

[16] Ganeriwal, S., Balzano, L., Srivastava, M.: Reputation-based framework for high integritysensor networks. ACM Trans. Sen. Netw. (2008)

[17] He, Q., Wu, D., Khosla, P.: Sori: A secure and objective reputation-based incentive scheme for ad hoc networks. In: Proceedings of IEEE Wireless Communications and Networking Conference, pp. 825–830 (2004)

[18] Kamvar, S., Schlosser, M., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: Proceedings of the 12th international conference on World Wide Web, pp. 640–651 (2003)

[19] Liang, Z., Shi, W.: Pet: A personalized trust model with reputation and risk evaluation forp2p resource sharing. In: HICSS 2005: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS 2005) - Track 7. IEEE Computer Society, Los Alamitos (2005)

[20] Zhan, G., Shi, W., Deng, J.: Poster abstract: Sensortrust a resilient trust model for wsns. In: SenSys 2009: Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (2009)