Trust-Based Secure And Energy Efficient Routing Framework For WSNS

Dhanunjayudu.K[#1], Mahesh.B[*2]

[#1]*M.Tech, Computer Science Engineering, Dr.KVSRIT Kurnool, Andhra Pradesh, India*
[#]*Assistant Professor, Department of CSE, Dr.KVSRIT, Kurnool, Andhra Pradesh, India*

Abstract--Identity deception is while replying routing information is one of the security threats in Wireless Sensor Networks (WSNs). As the nodes WSN are resource constrained, many attacks are possible. For instance an adversary might exploit the vulnerabilities WSN and launch attacks which disrupt normal functionalities of routing protocols. The attacks launched are generally wormhole attacks, sinkhole attacks and Sybil attacks. The mobility nature of network and other network conditions may make the situation even worse. These attacks can't be prevented with traditional cryptographic primitives as cannot be directly used with WSN. Therefore a special design for WSN is required in order to make it robust, trust-aware and secure. Recently Zhan, Shi and Deng proposed a trust – aware routing framework for WSNs. This framework energy efficient and trustworthy routing and avoid attacks on WSN. In his paper we implement such routing framework which is trust-aware and routes data securely. We built a prototype application to demonstrate the proof of concept. The empirical results revealed that he prototype is very effective in securing WSN from various attacks.

Index Terms – WSN, secure routing, trust-aware

I. INTRODUCTION

Wireless Sensors Networks (WSNs) have become popular in real world scenarios. These networks are essential to sense of monitor environments. They are very handy in various situations. For instance military can use it to monitor unmanned areas so as to know the movements of people there. The WSNs are ideal for any such application that monitors environment [1]. Applications of WSN include fire or forest monitoring, military surveillance, home surveillance, reporting any events that are detected. A WSN is made up of nodes that are battery powered. For this reason the nodes in WSN are energy constrained with less processing capabilities. The WSN are essentially multi-hop in nature as they need to have cooperative communications with sink or base station. The multi-hop routing in WSN has become target to adversaries as it gives scope to intrude into the network. Attacker may also tamper nodes, drop routes, cause traffic collision, jam communication channels [2] and so on. In this paper, we focus on the attacks launched by adversaries that misdirect network traffic. In other words we focus in the attacks that target routing information through identity deception. The hard to detect attacks that are made include Sybil attacks, sinkhole attacks and selective forwarding attacks [3]. These attacks are made simply using replay techniques used by adversaries. The worm hole attack is the attack made though malicious nodes that overhear wireless transmissions of valid node and also collude with other nodes [4].

Forgery of identity is another problem WSN. This will allow launghi8ng attacks pertaining to identity deception. With this a malicious node can misdirect the traffic of the network. A malicious node, for instance, can drop messages or send messages to an unintended server which is being maintained by hacker or adversary. For this reason it is essential to have monitoring about the packet delivery. Sinkhole attack is also made through stolen identity. In this attack a malicious node announces itself as valid sink node so as to get valuable and sensitive information from to other nodes in the network [5]. When such attack deceives more than half of the traffic, then that attack is known as black hole attack. Thus the attackers can use multiple identifies to have more attacks on the network. With every attack, they intend to take private or personal information for monetary another gains. Replaying routing information is very harmful to WSN in the real world. The mobility nature of WSN makes it more vulnerable. In WSN for efficient data collections various methods were proposed in [6], [7], [8], and [9]. Poor network conditions also cause problems in WSN as the attacker can compromise an honest node and take advantage from it.

Unfortunately, most existing routing protocols for WSNs either assume the honesty of nodes or focus on energy efficiency [10], or attempt to exclude unauthorized participation by encrypting data and authenticating packets. Examples of these encryption and authentication schemes for WSNs include TinySec [11], Spins [12], TinyPK [13], and TinyECC

[14]. Admittedly, it is important to consider efficient energy use for battery powered sensor nodes and the robustness of

The most existing routing protocols have common faults. However, they should consider security has their highest goal. A malicious node in WSN can cause havoc to network. The attacks are made through identity deception. Some routing protocols which are based on gossiping perform well against that for forwarding packets and choosing selective neighbors [15]. However, they are not energy efficient.

For security trust based approaches and cryptographic approaches are available. With trust based approach efficient routing is possible. By considering trust level of a node, it can take decisions thus making the network more secure. The trust based approaches are explored in [16], [17], [18] and [19]. Based on trust secure routing solutions are explored in [20] and [21]. Recently in [22] a framework was proposed to protect WSN from various attacks such as selecting forwarding attack, wormhole attack, sinkhole attack, black hole attack and Sybil attack. The framework focuses on secure routing in WSN. Trust awareness and synchronization are the main concepts through which they proposed the framework. In this paper we also implement such framework with a prototype application to demonstrate the efficient of the approach. The remainder of the paper is structured as follows. Section II provides review of literature. Section III provides details about the proposed system. Section IV presents experimental results while the section V concludes the paper.

II. RELATED WORKS

In the literature, it if found that WSN is vulnerable for Sybil attacks, sinkhole and wormhole attacks. These attacks are made based on the identity deception. The counter measures to these attacks are generally either known geographic information or synchronization [3]. A secure routing protocol that is based on feedback is explored in FBSR [23]. Its approach is statistics based to discover genuine nodes, compromised nodes and base stations. Trust aware security is explored in [24] which are evaluated with simulations. There are many existing routing solutions such as reputation and trust based systems. They can effectively avoid identity deception based attacks as they made decisions based on the trust value of the nodes in WSN. Two such systems in the literature are TARP [20] and ATSR [21]. However, they both can't provide security against identity deception attacks. Out of them the ATSR [21] is a trust aware routing protocol that can be used with large WSNs. The trust model used in ATSR has direct and indirect trusts. The trust values of nodes are considered while forwarding data to other nodes. This will prevent misforwarding attack and also prevents acknowledgements spoofing. TARP is another trust aware protocol which uses part routing behavior which also supports likability for determining effective paths.

III. PROPOSED TRUST AWARE ROUTING FRAMEWORK

The proposed routing framework is meant for securing communications in WSN. The nodes in the WSN should be able to have secure and genuine communications with base station. The network should not allow any attacks pertaining to identity deception. The framework prevents attacks such as Sybil, wormhole and sinkhole. This is achieved by considering trust values of nodes before making decisions on data forwarding. When any node is compromised that node can't have higher trust value and thus it can't participate in communications. We consider a multi-hop WSN for the experiments. The WSN we use for experiments is as shown in figure 1.

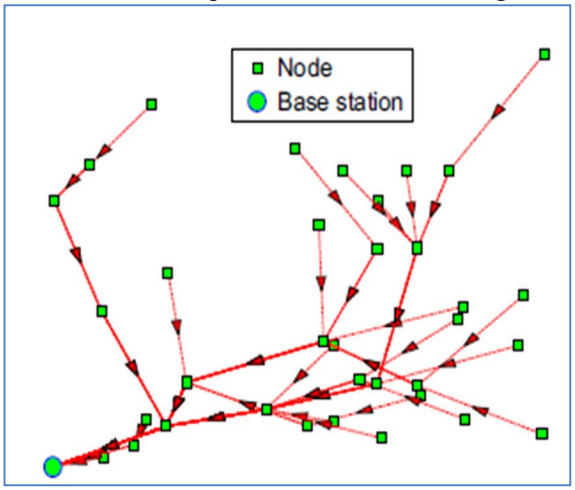

Fig. 1 – Multi-hop routing for data collection in WSN (excerpt from [22])

As seen in figure 1 the network is of multi-hop kind as there is cooperative communication between the nodes in the network. All sensor nodes are geographically scattered and they are sending environment information to the base station. It is the typical scenario in which we made our simulations. In this framework we made some assumptions. For instance we focus on only data collection part of the network. A sensor node is assumed to sense data and sends it to base station. There might be number of

base stations. Our approach works with any number of base stations. The main goal of the framework is achieving high throughput and protecting network from various identity deception based attacks besides energy efficiency. The important activities in the proposed system are presented din figure 2.

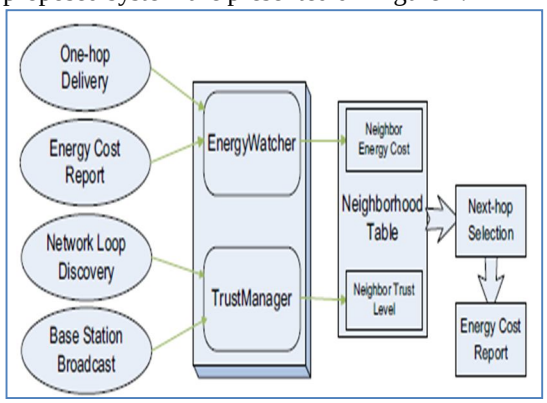

Fig. 2 – Important Components of proposed framework (excerpt from [22])

As can be seen in figure 2, it is evident that energy watcher monitors one-hop delivery, and energy cost report and estimates neighbor's energy cost. The trust manager takes network loop discovery and also base station broadcast and stores it into neighborhood table. In the neighborhood table neighbor energy cost and neighbor trust level is stored. These two are used to make intelligent decisions. Thus the proposed system is made energy efficient and secure besides improving throughput. Energy watcher computer energy level as follows.

$$E_{Nb} = \frac{E_{unit}}{p_{succ}} + E_b$$

The trust manager computes trust level of each neighbor based on various events such as broadcast nature of base station, trust level of each neighbor and discovery of network loops. The trust level is computed as follows.

$$T_{new\_Nb} = \begin{cases} (1 - w_{degrade}) \times T_{old\_Nb} \\ +w_{degrade} \times DeliveryRatio, \\ \text{if } DeliveryRatio < T_{old\_Nb}. \\ \\ (1 - w_{upgrade}) \times T_{old\_Nb} \\ +w_{upgrade} \times DeliveryRatio, \\ \text{if } DeliveryRatio >= T_{old\_Nb}. \end{cases}$$

Trust manager provides complete security to the communications in WSN. This is possible as the trust manager can determine the trust level of nodes and make appropriate routing decisions. Adversaries can't reach base station as they do not have trust.

IV. EXPRIMENTAL RESUTLS

We built a prototype application to demonstrate the proof of concept. The experiments are made through custom simulations in terms of number of delivered packets, number of nodes with delivery record, CTP without adversaries, with adversaries, and experiments to demonstrate attacks. The results of experiments are shown in this section in the form of a series of graphs.

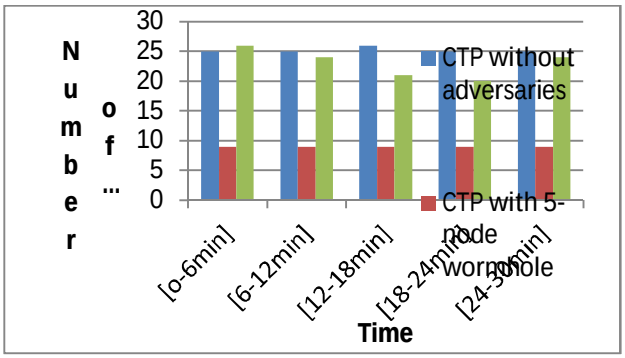

Fig. 1 – Time vs. number of nodes with delivery record (First Floor)

As can be seen in figure 1, the time is represented by horizontal axis while the number of nodes with delivery record is represented by vertical axis. The experiments are made with proposed framework. The collection tree routing protocol is also used for experiments with and without adversaries. The results reveal that the number of nodes with delivery records is more when there are no adversaries.

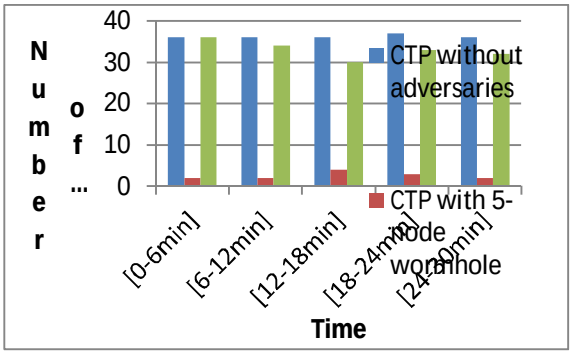

Fig. 2 – Time vs. number of nodes with delivery record (Second Floor)

As can be seen in figure 2, the time is represented by horizontal axis while the number of nodes with delivery record is represented by vertical axis. The experiments are made with proposed framework. The collection tree routing protocol is also used for experiments with and without adversaries. The results

reveal that the number of nodes with delivery records is more when there are no adversaries.

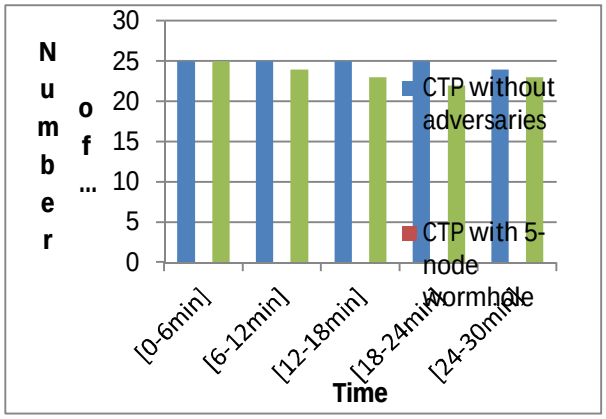

Fig. 3 – Time vs. number of nodes with delivery record (Third Floor)

As can be seen in figure 3, the time is represented by horizontal axis while the number of nodes with delivery record is represented by vertical axis. The experiments are made with proposed framework. The collection tree routing protocol is also used for experiments with and without adversaries. The results reveal that the number of nodes with delivery records is more when there are no adversaries.

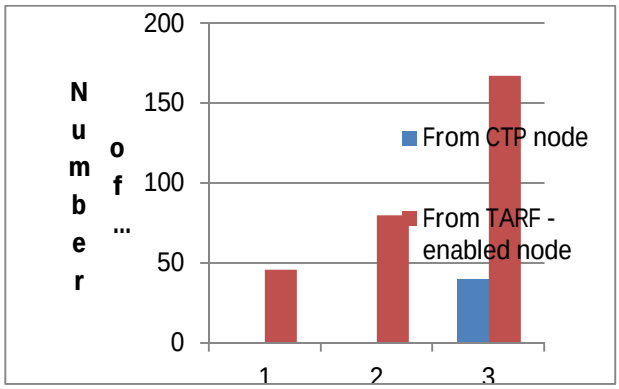

Fig. 4 – Number of reported detections

As can be seen in figure 4, it is evident that the number of reported detections is more with our framework enabled CTP node. This will prove the efficiency of the proposed framework when compared with normal CTP.

V. CONCLUSION

In this paper we studied the problem of security in WSNs. WSNs are vulnerable as they are open, resource constrained and mobility in nature. They are subjected to various attacks such as wormhole attack, sinkhole attack and Sybil attacks. Adversaries replay the routing information in order to launch these attacks. We implemented trust – aware routing framework that ensures that these attacks are prevented. The proposed framework is both trustworthy and energy efficient. A node in the network can track of trustworthiness of neighbors so as to take effective routing decisions. We built a prototype application to demonstrate the efficiency of the proposed framework. Experimental results reveal that he trust aware framework is very effective and useful for real world applications.

REFERENCES

[1] F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*. Morgan Kaufmann Publishers, 2004.

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

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

[4] 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 Telecommunication Technologies (ACT '09)*, 28-29 2009, pp. 555 –558.

[5] 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 Mobile Computing, Networking and Communications(WIMOB '08)*, 12-14 2008, pp. 526 –531.

[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 Communication Technology (ICACT 2008)*, vol. 1, 17-20 2008, pp. 75 –78.

[7] 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, 12-14 2005, pp. 22 – 26.

[8] L. Zhang, Q. Wang, and X. Shu, "A mobile-agent-based middleware for wireless sensor networks data fusion," in *Proceedings of Instrumentation and Measurement Technology Conference (I2MTC '09)*, 5-7 2009, pp. 378 –383.

[9] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in

Proceedings of the 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009), 20-24 2009, pp. 16 –19.

[10] 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.

[11] C. Karlof, N. Sastry, and D.Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proc. of ACM SenSys 2004*, Nov. 2004.

[12] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," *Wireless Networks Journal (WINET)*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[13] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*. New York, NY, USA: ACM, 2004, pp. 59–64.

[14] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 7th international conference on Information processing in sensor networks (IPSN '08)*. IEEE Computer Society, 2008, pp. 245–256.

[15] 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.

[16] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in *Proceedings of Aerospace Conference*, 2004.

[17] 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.

[18] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, "Trust based routing for misbehavior detection in ad hoc networks," *Journal of Networks*, vol. 5, no. 5, May 2010.

[19] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile ad hoc networks,"*Wirel. Netw.*, vol. 16, no. 4, pp. 969–984, 2010.

[20] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in *IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007)*, 8-11 2007.

[21] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, and L. Besson, "Design and implementation of a trust-aware routing protocol for large wsns," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 2, no. 3, Jul. 2010.

[22] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "Fbsr: feedbackbased secure routing protocol for wireless sensor networks," *International Journal of Pervasive Computing and Communications*, 2008.

[23] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative trust-based secure routing against colluding malicious nodes in multi-hop adhoc networks," in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, Nov. 2004, pp. 224 – 231.

[24] 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.

AUTHORS

K.Dhanunjayudu, received his B.Tech. degree in Computer Science from JNT University, Anatapur, India, in 2010. Currently pursuing M.Tech in computer science and engineering at Dr.KVSR Institute of Technology, Kurnool, India.

B.Mahesh, Completed M.Tech(CSE) from JNTUA, Anantapur in 2011. Attended 2 International conferences & 1 National Conference. Area of interest is Network Security and Cloud Computing.