STEAR: Secure Trust-Aware Energy-Efficient Adaptive Routing in Wireless Sensor Networks

B. M. Thippeswamy, S. Reshma, V. Tejaswi, K. Shaila, K. R. Venugopal, and L. M. Patnaik

***Abstract*—Secure communication is one of the most critical challenging tasks in multi-hop Wireless Sensor Networks (WSNs). Routing protocols of WSNs are highly susceptible to various attacks, which replay the routing information through the malicious node and steal the identities of the valid nodes in a network. The malicious nodes forward the packets far away from the sink, increasing the packet drop ratio, that sluggishes overall network efficiency. In order to overcome this problem, we have designed and implemented a secure trust aware energy efficient adaptive routing (STEAR) for dynamic WSNs. This protocol provides secure, trustworthy and energy efficient routing for multihop networks. STEAR is designed with effective mechanisms to identify the malicious nodes using dynamic secret key (DSK) assignment, trust and energy monitoring, and packets flow status monitoring. Simulation results show that network efficiency and throughput are better and packet drop ratio is reduced compared to earlier works.**

***Index Terms*—Dynamic secret key (DSK), energy monitor, secure communication, trust monitor, WSNs.**

I. Introduction

To achieve trust aware routing in multihop environment in WSNs is one of the most challenging tasks. The malicious nodes divert the messages far away from the sink, create congestion and disrupt the communication channels through different overwhelming attacks [1]. Major attacks that affect the multi-hop routing are Sybil attack, Worm Hole attack and Sink Hole attack [2].

The effect of these three attacks brings down the network efficiency in both static and mobile sink environments. The impact of these attacks is more in mobile sink environments when compared to static sink networks [3]. These attacks may also cause irreparable damage to the minimum security levels in networks.

A. Motivation

Security is one of the important issues in WSNs. Secure communication in WSN improves network efficiency and throughput. In earlier works, trust and status supervision schemes consider the trust value and energy level of each node while transferring the data from the source to the sink. The attackers are still successful to replay the routing information to extract the valid identity. Thus, it is necessary to device a mechanism by considering dynamic secret key (DSK), packet flow status along with trust and energy requirement level to improve the network security, efficiency and throughput.

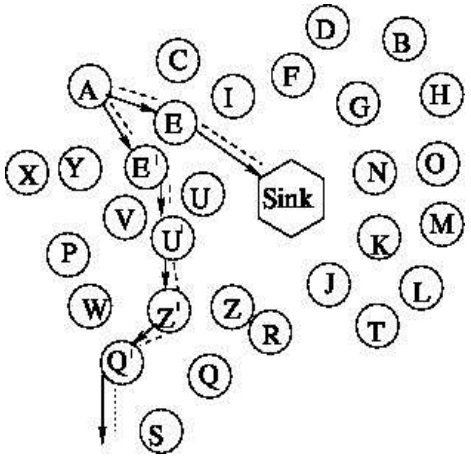

Fig. 1. STEAR mechanism.

These parameters are illustrated by using an example as shown in Fig. 1. Assume that an event has been generated at node A, then it begins to find a valid neighbour node to forward the packets towards the sink through one of its neighbours such as X, Y, E and C. The routing table of every node maintains the information like the trust level, the energy requirement to drive the packets towards sink, packet flow status and dynamic secret key (DSK) value of its neighbour nodes. To select a valid neighbour node, the node A considers the maximum trust value, minimum energy requirement, maximum packet flow status and valid DSK of its neighbour nodes. Node A identifies that one of its neighbour node E, (connected with thick line) has satisfied all these requirements. Thus, it selects node E as valid one and transfers the messages to the sink.

In earlier protocol trust aware routing framework (TARF), the neighbour node selection is based on only the trust level and energy requirement. But, in this case, the malicious node may also claim maximum trust level and minimum energy requirement to forward the packet. Thus, it cannot provide effective mechanism to identify the malicious node. Our protocol has considered two other parameters such as dynamic secret key Assignment and packet flow status to find the valid node. This situation can be observed in Fig. 1, assuming that, the node E´ claims the same identity of node E with maximum trust level and minimum energy requirement. Suppose the node A chooses node E´ as its neighbour then E´ diverts the packets far away from the sink through nodes U´, Z´ and Q´, and these packets will be lost.

Manuscript received October 10, 2014; revised April 15, 2014.

B. M. Thippeswamy is with the Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Anantpur, India (e-mail: bmtswamy@rediffmail.com).

S. Reshma, K. Shaila, and K. R. Venugopal are with the Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India (e-mail: Reshma229@in.com, shaila_ks@yahoo.com, venugopalkr@gmail.com).

V. Tejaswi is with the NIT, Suratkal, India (e-mail: tejaswikrv@gmail.com).

L. M. Patnaik is with the Indian Institute of Science, Bangalore, India (e-mail: lalitbr@gmail.com).

DOI: 10.7763/JACN.2015.V3.157

B. Contribution

We have designed a secure trust aware energy efficient adaptive routing protocol to forward the packets through more secure path from the source to the sink. The secure path is selected based on the four unique parameters, *viz:* (i) dynamic secret key *(*DSK) (ii) packet flow status (iii) energy requirement and (iv) trust level. The combination of these parameters maximizes the energy efficiency, network throughput and packet delivery rate.

C. Organization

The rest of the paper is organized as follows. A brief literature of related works is presented in Section II. Background work is discussed in Section III. Section IV defines the problem and objectives. Performance evaluation is presented in Section V. Concluding remarks are summarized in Section VI.

II. Literature Survey

This section presents a brief summary of related works.

Rezguin *et al*., [4] proposed Trust Aware Routing Protocol (TARP) for Sensor Actuator Networks (SANets) that helps to route the packets by detecting the past behavior of the nodes and link quality to determine the feasible efficient path. TARP is energy efficient and scalable for network traffic. The complete performance of the TARP can be analyzed only when it is applied to the specific applications related to the prioritized traffics.

Mario *et al*., [5] proposed wormhole based anti jamming techniques in sensor networks, where the attacker masks the event and jamming appropriate subset of nodes. This situation prevents the nodes from the reporting the sensed data to the network operator. This protocol exploits channel diversity in order to create wormholes that lead out of the jammed region. It has been achieved by using three concepts, namely wired pairs of sensors, frequency hopping and uncoordinated channel hopping. The process involves high time complexity.

In our proposed protocol, we have designed and implemented an efficient mechanism to find secure communication path from the source to the sink. The secure path computation includes four major prominent parameters i.e., trust level, energy requirement, packet flow status and dynamic secret key (DSK) generation and assignment. These parameters greatly improve the malicious node detection rate, energy efficiency, network throughput and packet delivery rate.

III. Background

Most of the existing trust aware frameworks use the common parameters such as, the trust level and energy requirements of the neighbor nodes to forward packets from the source to the sink. But the attackers continue to participate in replying the routing information and misdirect the packets far away from the sink.

In order to overcome this problem, the trust aware routing framework [TARF] [6] is designed for multihop wireless sensor networks. It identifies the malicious nodes based on the trust level and avoid replay of routing information. This algorithm has significantly improved the packet delivery rate. But it lags in the issues related to the load balancing, latency and fairness problems. TARF [7] is an extended work of aforementioned TARF [6], which has considered both trust level and energy requirement of neighbor node to forward the packets towards the sink. This algorithm is achieved better energy efficiency and latency with increased packet delivery rate and minimizes the latency. But, the problems related to load balancing and fairness have not completely resolved.

In our work we identified two unique and effective parameters: dynamic secret key (DSK) and packet flow status (P_s) along with the trust level and energy requirements. The trust level, energy monitor and packet flow status are defined as shown in the following equations (1), (2) and (3) respectively. These parameters collectively achieve more secure communication and results in better network throughput and efficiency.

$$T_l = T_l - \frac{\text{No of packet received by the sink}}{\text{No of packets sent from the source}} \tag{1}$$

$$E_r(i) = \frac{\text{packet}_{\text{size}} \times T_e}{\text{distance}(i, \text{sink})} \tag{2}$$

$$P_s = N_p \tag{3}$$

IV. Problem Definition

TABLE I: Secure Trust Aware Energy Efficient Adaptive Routing (STEAR) Algorithm

Algorithm: Secure Trust aware Energy efficient Adaptive Routing (STEAR) Algorithm
Step 1: Generate nodes Randomly
Step 2: Dynamic Secret Key (DSK) Generation and Assigning initial trust level
for i = 0 to N **do**
if *time* > *LUI* **then**
if *node-Id* **then**
DSK node-Id ← *int*(*rand*( ) ×250)
end if
end if
if *node-Id* **then**
T_l (*node-Id*) = 0.5
end if
end for
Step 3: Routing Table Maintenance
***Routing_Table_Maintenance*( )**
Step 4: Event Generation
Step 5: Identify Neighbor nodes
Step 6: Secure Path Calculation
***Secure_Path_Computation*( )**
Step 7: Repeat step 6 and 7 until it reaches sink
Step 8: Forward the packet through the secured path
for each *neighbour node* **do**
if $Q_l < Q_{threshold}$ && max R_e && min d && min D **then**
sendMessage( )
else if $Q_l > Q_{threshold}$ **then**
select next node
end if
end for
Step 9: Repeat above step until the reaches sink.

In a given wireless sensor network of N randomly deployed nodes, we consider four major parameters: trust level — $T_{l,}$ minimum energy requirement — $E_{r.,}$ dynamic secret key — DSK and packet flow status — P_s in secure path computation between the source node and the sink. Initially, a common trust value T_l is assigned to each node in the network and monitored by the trust monitor — T_M. The value of T_l decreases as the node drops the packets to be transmitted from the source to the sink. The DSK is dynamically generated and assigned to each node over stipulated time interval known as least update time interval (LUI). E_r represents the minimum energy required by each node to transmit the packet towards the sink and is monitored by energy monitor E_M. The packet Flow status of each node is represented by P_s, which reflects the value of number of packets transmitted by each node towards the sink over regular time intervals. The secure path computation involves the identification of valid neighbor node on the basis of combined values of maximum trust level T_l, minimum energy requirement E_M, maximum packet flow P_s and *DSK* matching. This computation process repeats to find all possible valid nodes from the source and the sink, and finally, the message transfer occurs through the secure path.

Our proposed algorithm is shown in the Table I.

V. Simulation and Performance Analysis

The STEAR protocol is simulated using NS-2 simulator. The energy efficiency, the packet delivery ratio and the Network Throughput are the major performance metrics used to analyse the performance of our protocol and the simulation results are depicted in the following sections. Simulation is carried out with 50 sensor nodes, which are randomly deployed over the area of 1000m × 1000m.

A. Performance Analysis

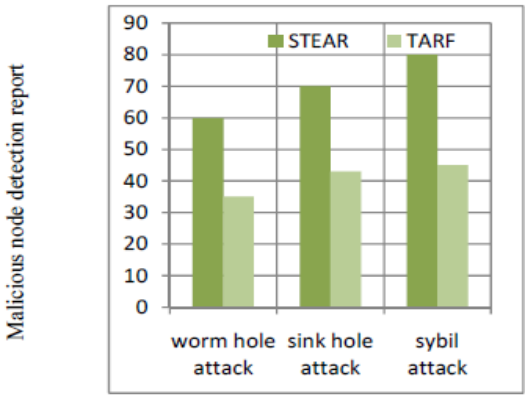

Fig. 2. Malicious node detection report references.

Fig. 2 illustrates the statistics of the malicious node detection by both STEAR and TARF protocols with respect to three most common attacks: Worm hole attack, Sink hole attack and Sybil attack. The graph clearly indicates that the STEAR detects more number of malicious nodes in all these cases when compared to TARF (42% - worm hole attack, 40% - sink hole attck and 44% - sybil attack). This is mainly achieved due to the consideration of unique parameter - dynamic secret key (DSK) assignment for each node at regular intervals.

VI. Conclusions

Secure communication is one of the major issues in WSNs due to the various types of attacks, which degrades the overall network efficiency. TARF considers only the trust level and energy requirement to forward the packets towards the sink. Our proposed algorithm, STEAR provides an efficient trust aware framework with most prominent and unique Parameters such as trust value, energy requirement, packet flow status and DSK value. The decision of valid node along with secure path is based on the combined values of these parameters. The trust value monitoring and packet flow status of each node reflects its legitimacy and acceptability towards secure communication. Energy requirement and trust level monitoring increases the probability of detecting the malicious nodes. The DSK is one of the major parameter that helps to diffuse the identity deception. Thus, our protocol enhances overall network efficiency with increased energy efficiency, network throughput and packet delivery rate. Further, this work can be extended for very large scale sensor networks.

References

[1] H. Huang, N. Ahmed, and P. Karthik, "On a new type of denial of service attack in wireless networks: The distributed jammer network," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2316-2324, July 2011.

[2] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941-954, July 2010.

[3] L. Bai, F. Ferrese, K. Ploskina, and S. Biswas, "Performance analysis of mobile agent-based wireless sensor network," in *Proc. Eighth International Conference on Reliability, Maintainability and Safety*, 2009, pp. 16-19.

[4] A. Rezgui and M. Eltoweissy, "TARP: A trust aware routing protocol for sensor-actuator networks," in *Proc. IEEE International Conference in Mobile Ad-Hoc and Sensor Systems*, 2007, pp. 1-9.

[5] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-based ant jamming techniques in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 100-114, January 2007.

[6] G. Zhan, W. Shi, and J. Deng, "TARF: A trust aware routing framework for wireless sensors," in *Proc. Seventh European Conference on Wireless Sensor Networks*, 2010, pp. 65-80.

[7] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust aware routing framework for Wsns," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184-197, March/April 2012.

B. M. Thippeswamy is an associate professor and the head of the Department of Computer Science and Engineering at Sambhram Institute of Technology, Bangalore, India. He obtained his B.E degree in computer science and engineering from Mysore University and the M.E degree in computer science and engineering from Bangalore University, Bangalore. He is presently pursuing his PhD degree in the area of wireless sensor networks in JNTU Anantpur, India. His research interest is in the area of wireless sensor networks.

S. Reshma is an assistant professor in the Department of Computer Science and Engineering at Sambhram Institute of Technology, Bangalore, India. She received her bachelor's degree in computer science and engineering from Visvesvaraya Technological University and the master of technology degree from Visvesvaraya Technological University, Regional Center, Bangalore. Her research interest is in the area of wireless sensor networks.

V. Tejaswi is a M.Tech student in the Department of Computer Science and Engineering, National Institute of Technology, Surathkal. She completed her B.Tech degree in computer science and engineering from R V College of Engineering, Bangalore. Her research interest is in the area of wireless sensor networks

K. Shaila is a professor and the head of the Department of Electronics and Communication Engineering at Vivekananda Institute of Technology, Bangalore, India. She obtained her B.E degree in electronics and her M.E degree in electronics and communication engineering, and the PhD degree from Bangalore University, Bangalore. Her research interests are in the area of sensor networks, Adhoc networks and image processing.

K. R. Venugopal is currently the principal of University Visvesvaraya, College of Engineering, Bangalore University, Bangalore. He obtained his bachelor degree in engineering from University Visvesvaraya College of Engineering. He received his master's degree in computer science and automation from Indian Institute of Science Bangalore. He was awarded the Ph.D. degree in economics from Bangalore University and the Ph.D. degree in computer science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in electronics, economics, law, business finance, public relations, communications, industrial relations, computer science and journalism.

He was a postdoctoral research scholar at University of Southern California, USA. He has authored and edited 49 books on computer science and economics, which include petrodollar and the world economy, C aptitude, mastering C, microprocessor programming, mastering C++ and digital circuits and systems etc.. During his three and half decades of service at University Visveraya College of Engineerng. He has over 300 research papers to his credit. His research interests include computer networks, wireless sensor networks, parallel and distributed systems, digital signal processing and data mining.

L. M. Patnaik is currently an honorary professor of Indian Institute of Science, Bangalore, India. He was a vice chancellor of Defense Institute of Advanced Technology, Pune, India and was a professor since 1986 with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 35 years of his service at the institute he has over 700 research publications in refereed international journals and refereed international conference proceedings. He is a fellow of all the four leading Science and Engineering Academies in India; a fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high performance computing and soft computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD, soft computing and computational neuroscience.

Computer Information Technology