IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 2, February 2015.
www.ijiset.com
ISSN 2348 – 7968

A Trust Supervision in Unattended WSN using Novel Approaches

G.Bakkiyaraj[1], R.Shanthipriya[2]

P.G Student, Department of CSE
Roever Engineering College, Perambalur, India.

Abstract

The Unattended Wireless Sensor Networks (UWSNs) are described by extensive periods of incoherent operation and fixed or unequal intervals between sink visits. The deficiency of an online trusted third party implies that existing WSN trust Supervision schemes are not applicable to UWSNs. A trust Supervision system for UWSNs to provide capable and robust trust data storage and trust production, for trust data storage, we utilize a geographic hash table to recognize the storage nodes and to appreciably decrease the storage cost. We use one-sided logic based compromise techniques to moderate trust fluctuations caused by environmental factors. We develop a set of trust similarity functions to detect trust outliers and to maintain trust pollution attacks. We make obvious, through general analyses and simulations, that the proposed scheme is proficient, robust and scalable.

Key Words: *Unattended wireless sensor network (UWSN), trust Supervision, one-sided logic, Trust data Storage.*

1. Introduction

The Wireless Sensor Network has been used in challenging, unfriendly environments for various applications such as forest fire detection, battlefield surveillance, habitat monitoring, traffic supervision, etc. One common assumption in conventional WSNs is that a trusted third party, e.g., a sink, is always available to collect sensed data in a near-to-real-time fashion.

Although many WSNs operate in such a mode, there are WSN applications that do not fit into the real time data collection model. Consider an example of a monitoring system deployed in a natural park to detect poaching activities. The lack of regular access routes and the size of the surveillance area would require a mobile sink to collect data periodically. Another example [9] is an underwater mobile sensor network for submarine tracking and harbor monitoring. The inaccessibility of the protected area and other technical problems make it difficult to maintain continuous connections between sink and sensors. Fig. 1 shows an example of Unattended WSNs (UWSNs) with a mobile sink visiting the network at either fixed or irregular intervals to collect data.

Trust Supervision becomes very important for detecting malicious nodes in unattended hostile environments. It can also assist in secure routing, secure data distribution and trusted key exchange. An efficient trust supervision system is required to handle trust related information in a secure and reliable way. It should deal with uncertainty caused by noisy communication channels and unstable sensor behavior. We propose a trust Supervision scheme for efficient trust generation as well as scalable and robust trust data storage in UWSNs. A central issue for trust Supervision in UWSNs is how to store trust data without relying on a trusted third party. Initially, we consider two simple trust Supervision schemes as a first-step attempt to address the existing trust storage problems in UWSNs. After analyzing the shortcomings of these simple schemes, we propose an advanced scheme based on a Geographic Hash Table (GHT). Our advanced scheme allows sensor nodes to put and *get* trust data to and from designated storage nodes based on node IDs.

Sensor nodes do not need to know the IDs of storage nodes. They use a hash function to find locations of the storage nodes, which significantly reduce the storage cost. We also propose a set of similarity threshold functions to remove outliers from trust opinions. This prevents attackers from generating false trust opinions and from polluting trustworthiness.

The rest of the paper is organized as follows. Related work is reviewed in Section. The Section defines the network scenario, security model and design goals. Section 4 presents some background material on trust Supervision in sensor networks [2][4] and on subjective logic. Section 1 introduces our solutions for efficient trust data storage. Section 2 reports a simulation-based study conducted to evaluate the efficiency and the robustness of the proposed schemes. Section considers advanced approaches to reliable trust generation. Section is offers conclusions.

The threshold function is expected to neutralize false trust opinions as much as possible. It is also desirable to reduce false positives (when trust opinions are considered as false trust opinions even though they are correct)[3], as well as false negatives (when trust opinions are considered as correct trust opinions even though they are false). Therefore, we aim to increase true positives as much as possible while keeping very few false positives and false negatives the simulations and discussions in the previous section, we have demonstrated that AS significantly reduces storage cost caused by distributed data storage and provides resilience to *ADV_Del*. To analyze the data storage event is possible to Wireless Sensor networks in portable event handling method of hostile network.

ISSN 2348 – 7968

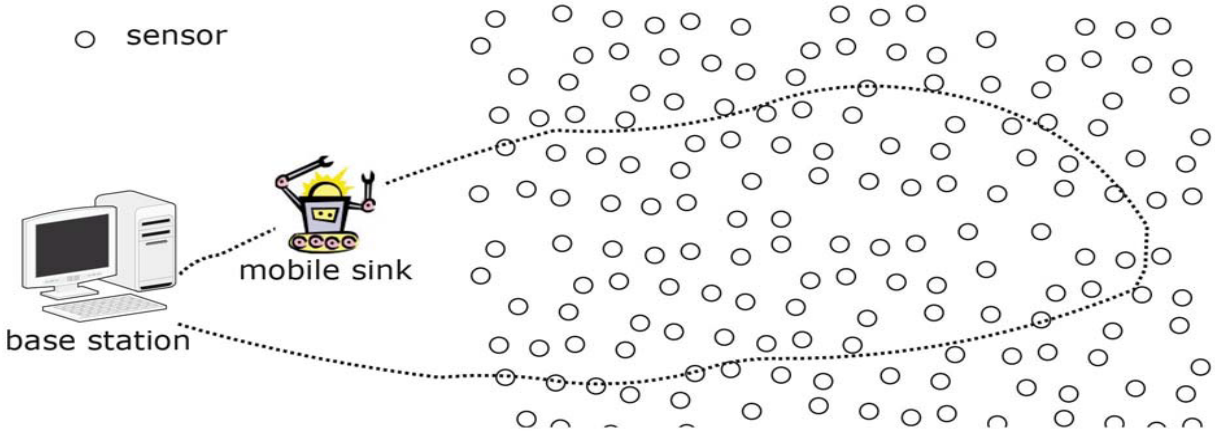

Fig.1 examples of UWSN

2. Related Works

In this section, we review the existing trust Supervision schemes in WSNs, ad hoc and P2P networks.

2.1 Basic Trust supervision in WSN

Several solutions have been recently proposed for trust Supervision in WSNs. In the authors designed a protocol to diagnose and mask arbitrary node failures in an event-driven WSN. In, the authors proposed a Bayesian trust Supervision framework where each node maintains reputation metrics to assess past behavior of other nodes and to predict their future behavior. The temporary point is proposed iTrust, integrated trust [3] framework for WSNs. A trust aware routing protocol for WSNs was proposed. The protocol exploits prior routing patterns and link quality to determine efficient routes. In the authors proposed a trust-based routing scheme that selects a forwarding path based on the trust requirement of a packet and the trust level of neighbor nodes.

2.2 Trust supervision in Ad Hoc Networks

In More trust Supervision studies were conducted in the field of ad hoc networks. The authors in proposed a reputation system based on Bayesian estimation of misbehavior in mobile ad hoc networks. The work in introduced an information theoretic framework to measure trust and to model trust evolution [13]. A data-centric framework for trust establishment was proposed in. In the authors proposed a distributed trust scheme based on distributed public key certificate Supervision for mobile ad hoc networks.

2.3 Trust supervision in P2P Networks

The authors in proposed a Peer-Trust model based on public key infrastructure and trust propagation. Power trust, a robust and scalable P2P reputation scheme, was proposed to leverage the power-law feedback factors. In the authors developed Credence, a decentralized object reputation and ranking system for P2P networks. UWSNs are an emerging class of wireless networks. The authors in also defined a mobile adversary and proposed a set of schemes to neutralize attacks focusing on erasing data. Techniques providing forward secrecy and backward secrecy of data stored in sensors are explored [5][6]. To the best of our knowledge, our earlier work is the first study which proposed trust data storage and trustworthiness calculation to facilitate trust Supervision in UWSNs. In this paper, we further proposed a set of schemes to mitigate trust pollution attacks based on subjective logic and various trust similarity measures. Most of the trust Supervision solutions developed for traditional WSNs, however, rely on the presence of an online trusted third party, e.g., to store and distribute trust data. They cannot be applied directly to UWSNs due to the absence of the sink (or the base station). Is one exception that proposed a distributed scheme establishing reputation-based trust among sensor nodes? The authors anyhow did not consider significant trust attacks (as defined in Section, [7] against the generated trust. The work in addressed data centric storage in WSNs, but trust Supervision and security attacks are not considered.

2.4 Security Model

The UWSNs can be attacked in many ways. In this study, we focus on an adversary *ADV* launching attacks against trust data2. We divide the attacks into two categories: *trust eraser* and *trust pollution* attacks. The effect of the trust eraser attack (denoted as *ADV_Del*) is that the trust data stored in sensors are lost and cannot be retrieved by trust consumers. For instance, *ADV* could try to compromise sensors and to erase the trust data stored in them.

ISSN 2348 – 7968

Moreover, when sensors are nonfunctional [15][17](e.g., due to energy depletion, natural disasters, etc.)

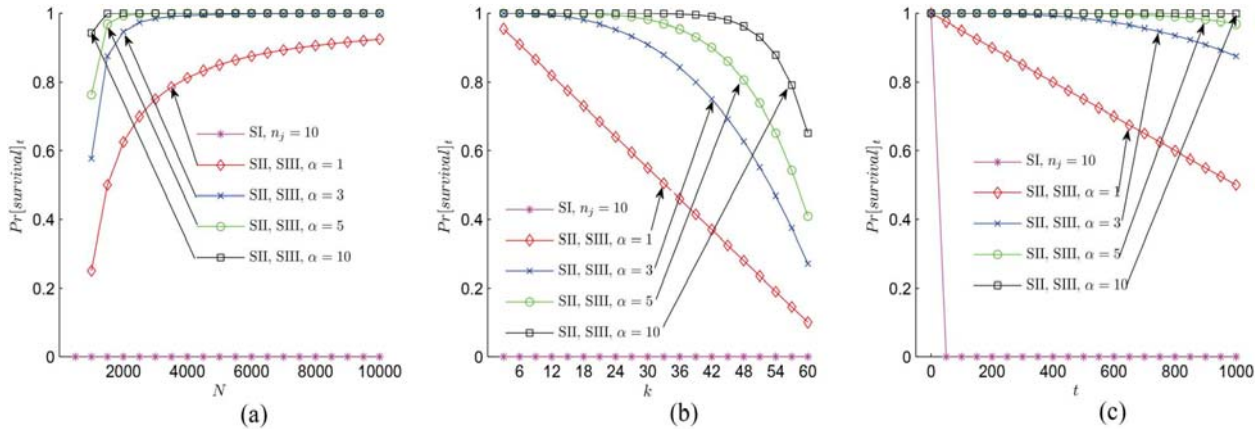

Fig.2 Comparison of SI, SII and AS

3. Proficient and Robust Storage of Conviction Data

In traditional WSNs, a trusted third party, e.g., base station, is used to keep and calculate received trust opinions. The queries of sensors' trustworthiness are also sent to and answered by the base station. However, since UWSNs do not have a base station [18], trust opinions of sensors need to be stored in sensors instead. Therefore, once sensor *bi* generates an opinion *Tj, ti* at time interval *t*, it either stores *Tj, ti* locally or sends *Tj, ti i* to other nodes. Next we consider three trust data storage schemes without involving the base station. First, we introduce two basic schemes and discuss their shortcomings. Then we propose an advanced scheme to improve the basic schemes.

3.1 Basic Scheme I (SI) - Trust Data Local Storage

The main idea of the SI is to keep generated trust opinions locally, i.e., *bi* generates *Tj, ti* and then stores *Tj, ti* in its own memory. In other words, *bi* is not only one of *sj*'s trust producers but also one of *sj*'s trust managers. The SI includes local storage of trust opinion, and trust opinion querying and calculation:

1. *Local storage of trust opinion.* At every time interval, each sensor generates trust opinions about its neighbor nodes, combines it with previous trust opinions according to Eq. (2) and stores it locally. Note that the generated trust opinions are combined as a combined trust opinion resulting in very low storage cost. For instance, *bi* generates *Tj,t*1*i* , *Tj,t*2*i* and *Tj,t*3*i* at *t*1, *t*2 and *t*3, respectively, and stores the combined trust opinion in its memory as *Tji* = *Tj,t*0∪*t*1∪*t*2∪*t*3*i*.
2. *Trust opinion querying and calculation*. Consider the example in Fig. 2. Assume that sensor *sa* wants to estimate the trustworthiness *ϒj* of another sensor, *sj*. It broadcasts a trust opinion request; *ASK (Tj∗)*, to ask sensors to collect opinions of other sensors about *sj*. Here, we assume a suitable broadcast authentication protocol, e.g., multilevel μTESLA [34], for secure and reliable transmission of such broadcast values. If there is no direct relationship between two sensors (e.g., *sh* and *sj*), they have highest uncertain opinion score about each other's trustworthiness, i.e., *Tjh= Thj*= {0, 0, 1}.receiving *ASK (Tj∗)*, each sensor sends feedback messages, *ANS (Tj∗)*, to *sa* if they have a direct relationship with *sj*. Otherwise they just drop *ASK (Tj∗)*. Next, *sa* combines received sensors' opinions using a consensus operator (Eq. (1)) to compute *sj*'s trustworthiness *ϒj*, and stores the results.

Proposition1. In the Basic Scheme I, the probability that at least one trust manager node remains uncompromised within t time intervals is

$$Pr\,[survival]^j_t = 1,\ k * t < nj$$

$$Pr\,[survival]^j_t = 0,\ k * t \geq nj$$

Where nj is the number of neighbor nodes and k is the compromising capability of ADV as defined in Section 1.

3.2 Basic Scheme II (SII) - Distributed Trust Data Storage

In order to address the shortcomings of the SI, we should ensure that: (1) a sensor *sj*'s trust producer and trust manager is not the same node; (2) *ADV* cannot easily find trust manager nodes; and the scheme is resilient against

ISSN 2348 – 7968

node failures. A straightforward solution would be to data are lost and are considered as non-recoverable in this specify for each node a designated trust manager node that stores its trust data. The trust manager should not be one of the node's direct neighbors. The components of the SII scheme are defined as follows.

3.3 Advanced Scheme (AS)

Our Advanced Scheme (AS) utilizes a hash-table-like interface of GHT [10] where nodes can *put* and *get* data based on their data type, i.e., *Put (Data Type, Data Value)* and *Get (Data Type)*. Since a sensor ID is unique in the network, trust producers are able to *put* trust opinions to trust managers based on the ID, i.e., *Put (sj, Tj, ti)*. Trust consumers are able to *get* trustworthiness from trust managers using the same sensor ID, i.e., *Get (sj)*. In other words, trust opinions are pushed by, and stored at the same trust manager node. The normal abortionist is created.

Meanwhile it enables trust consumers to pull trustworthiness from the trust manager nodes consistently. Neither trust producers nor trust consumers need to store the IDs of trust manager nodes, reducing storage cost significantly. Furthermore [11], the scheme should not be sensitive to node failures. That is, the scheme should be resilient to *ADV_Del*. Thus [4], trust opinions are pushed to α ($\alpha > 1$) trust manager nodes, whereas trust consumers pull trustworthiness from α trust managers. To do so, we modify the original basic operations of GHT. The communication model is executed when the operation is moderated for each and every node. It will allocate the space for transmitting the signal propagation through the network model configuration.

study. The communication network process is a peer to peer network analyze, it organize the data transmission

4. Effectiveness and Robustness Estimation

In this section we conduct a set of simulations in MATLAB to show that AS has the strongest performance among these three schemes in terms of both efficiency and robustness. We consider an UWSN where 10000 nodes are randomly distributed in a 3000×3000 unit's area. The other parameters are set as follows. Each sensor has transmission range φ = 150 units. *ADV_Del* has compromising capability k = 25. The number of trust managers nodes α = 3. The simulation results are averaged over 20 randomly deployed networks and are explained below. Fig. 3(a)–(c) show the performance of t in terms of how many intervals the network can survive, given different α, k and φ. It demonstrates that SII and AS have better performance than SI does with respect to t for all values of α, k and φ. We observe in Fig. 3(a) that increasing α improves the performance of t. Meanwhile, increasing k decreases the performance of t. Fig. 3(c) shows that φ has no impact on SII and AS in terms of t but slightly increases the performance of t in SI. Since *ADV_Homo* tries to either increase Υ or decrease Υ monotonously, we conduct two simulations. In the first simulation, *ADV_Homo* is assumed to generate false trust opinions *fT* to increase Υ. In contrast, *ADV_Homo* is set to decrease Υ in the second simulation. In order to increase Υ, *ADV_Homo* increases B and decreases D simultaneously. That is, generate *fT* that satisfies $E(cB) < E(fB)$ and $E(cD) > E(fD)$. We select a special case when cT = {0.1, 0.3, 0.6}, fT = {0.4, 0.1, 0.5} and $\sigma c = \sigma f$ = 0.01.

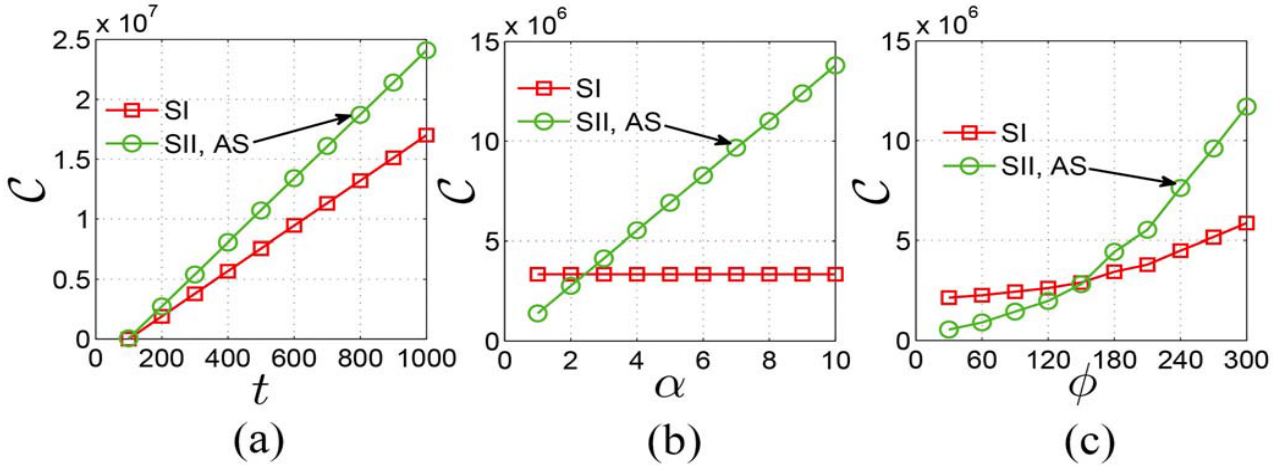

Fig.3 Replication results: $t/\alpha/\varphi$ vs. C.

Fig. 3(a)–(c) display the performance in terms of communication cost C for different α, k and φ. Distributed trust data storage is resilient to *ADV_Del* and provides higher t. However, it causes higher communication costs. As shown in Fig. 3(b) and (c), the communication cost is acceptable if $\alpha \leq 3$ and $\varphi \leq 120$. The work presentation

ISSN 2348 – 7968

needs to analyze the initial calculation and it provides the values for primary storage recognition [16]. In addition to inform the logic based process is established in overall network configuration in a Wireless Sensor Networks.

In this paper, conclude a relative of proficient and robust trust supervision schemes for UWSNs based on Subjective Logic. Our advanced trust storage scheme, AS, facilitates distributed trust data storage to ensure high reliability of trust data. It takes the advantage of both GHT and GPSR routing to find storage nodes and to route trust data. We have also proposed several methods to moderate trust pollution attacks based on different trust relationship measures. It established that our trust Supervision schemes are durable to major attack categories including *ADV_Del*, *ADV_Noise*, *ADV_Homo*, and *ADV_Hbd*. Moreover, our recreation results established that AS has much lower storage costs compared with the less complicated approaches.

6. Future Enhancements

To Combine AS with resemblance verge measures, we are able to extensively reduce trust storage costs in future and perform proficient node withdrawal and mitigation of *ADV*'s pollution attacks is possible.

Acknowledgment

This research work was supported and sponsored by my Head of the department Mr.K.Sivakumar through University project preparation, Department of Computer Science, Roever Engineering College, Perambalur, India.

References

[1] Ma, C. Soriente, and G. Tsudik, "*New adversary and new threats: Security in unattended sensor networks*," *IEEE Netw.*, vol. 23, no. 2, pp. 43–48, Mar. 2009.

[2] Y. Ren, V. Oleshchuk, F. Y. Li, and S. Sulistyo, "*SCARKER: A sensor capture resistance and key refreshing scheme for mobile WSNs*," in *Proc. IEEE LCN*, Bonn, Germany, 2011.

[3] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "*Catch me (if you can): Data survival in unattended sensor networks*," in *Proc. IEEE PERCOM*, Hong Kong, 2008.

[4] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "*United we stand: Intrusion-resilience in mobile unattended WSNs*," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1456–1468, Jul. 2013.

[5] R. Di Pietro and N. Verde, "*Epidemic data survivability in unattended wireless sensor networks*," in *Proc. ACM WiSec*, Hamburg, Germany, 2011.

[6] K.-S. Hung, K.-S. Lui and Y.-K. Kwok, "*A trust-based geographical routing scheme in sensor networks*," in *Proc. IEEE WCNC*, Kowloon, Hong Kong, 2007.

[7] A. Rezgui and M. Eltoweissy, "*TARP: A trust-aware routing protocol for sensor-actuator networks*," in *Proc. IEEE MASS*, Pisa, Italy, 2007.

[8] Y. Ren, V. Oleshchuk, and F. Li, "*Optimized secure and reliable distributed data storage scheme and performance evaluation in unattended WSNs*," *Comput. Commun.* vol. 36, no. 9, pp. 1067–1077, May 2013.

5. Conclusion

[9] N. Lewis and N. Foukia, "*Using trust in key distribution in wireless sensor networks," in Proc. GLOBECOM Workshops*, Washington, DC, USA, 2007.

[10] S. Ratnasamy *et al.*, "*GHT: A geographic hash table for datacentric storage*," in *Proc. ACM WSNA*, 2002.

[11] M. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. Hu, "*TIBFIT: Trust index based fault tolerance for arbitrary data faults in sensor networks*," in *Proc. DSN*, 2005.

[12] S. Ganeriwal, L. Balzano, and M. Srivastava, "*Reputation-based framework for high integrity sensor networks*," *ACM Trans. Sen. Netw.* vol. 4, no. 3, pp. 1–37, May 2008.

[13] K. Yadav and A. Srinivasan, "*iTrust: An integrated trust framework for wireless sensor networks*," in *Proc. ACM SAC*, New York, NY, USA, 2010.

[14] S. Buchegger and J. Le Boudec, "*A robust reputation system for mobile ad-hoc networks*," in *Proc. P2PEcon*, 2004.

[15] Y. L. Sun,W. Yu, Z. Han, and K. Liu, "*Information theoretic framework of trust modeling and evaluation for ad hoc networks*," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[16] S. Shenker, S. Ratnasamy, B. Karp, R. Govindan, and D. Estrin, "*Data-centric storage in sensornets*," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 33, no. 1, pp. 137–142, 2003.

[17] M. T. Refaei, L. A. DaSilva, M. Eltoweissy, and T. Nadeem, "*Adaptation of reputation Supervision systems to dynamic network conditions in ad hoc networks*," *IEEE Trans. Comput.*, vol. 59, no. 5, pp. 707–719, May 2010.

[18] A. Becher, Z. Benenson, and M. Dornseif, "*Tampering with motes: Real-world physical attacks on wireless sensor networks*," in *Proc. Int. Conf. SPC*, York, U.K., 2006.

[19] http://sprout.ics.uci.edu/projects/uwsnwebpage/security_uwsn.html

[20] http://onlinelibrary.wiley.com/doi/10.1002/wcm.1042/abstract

G.Bakkiyaraj received the B.E Computer Science and Engineering degree from Oxford Engineering College, Anna University, Trichy, India, in 2013. He is currently pursuing M.E Computer Science and Engineering degree from Roever Engineering College, Anna University, Perambalur, India. He was presented the papers in Fifteen National Conferences and more number of International Conferences and also published the paper in various International Journals. He got many prizes from paper presentation in Conferences. His research interest includes image/video processing, Face identification, Pattern Recognition. He is the member of the IACSIT, IAETSD, IAENG, and UACEE.

S.Kanagavalli received the B.Tech Information Technology degree from Kalasalingam University, Srivilliputhur, India, and M.E Software Engineering degree from G.K.M College of Engineering, Anna University, Chennai, India. She was currently working as an Assistant professor in Department of CSE, Dhanalakshmi Srinivasan College of Engineering, Perambalur. She was presented the papers in more number of International Conferences. Her research interest includes Software Testing, Data Mining, Face identification, Pattern Recognition. She is the member of the ISTE.