International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-9 March-2013

A Bandwidth-Efficient Cooperative Authentication and an En-route Filtering Scheme for Filtering Injected False Data in Wireless Sensor Networks

T.R. Yashavanth[1], Ravi S Malashetty[2], Rashmi C.R[3]

Abstract

Injecting false data attack is a well-known serious threat to wireless sensor network, for which an adversary reports bogus information to sink causing error decision at upper level and energy waste in en-route nodes. In this paper, we propose a novel bandwidth-efficient cooperative authentication scheme for filtering injected false data. The proposed method of BECAN can save energy by considering the random graph characteristics of deployment of sensor node and a technique for cooperative bit-compressed authentication and this method is done by early detection and filtering most of injected false data at the en-route nodes with minor extra overheads. Further, it is necessary to check at the sink, a very small amount of injected false data which largely helps to reduce burden on the sink. For the proposed method, theoretical and simulation results are given which shows the effectiveness regarding high filtering and energy saving. We propose an EFSP (En-route Filtering Scheme based on Priority) to control the number of votes. The EFSP determines priorities through the fuzzy rule-based system. Base station sends priority to the cluster head and then according to the priority a specified number of votes are attached to the report by the cluster head.

Keywords

Wireless sensor network, injecting false data attack, random graph, EFSP, cooperative bit-compressed authentication.

1. Introduction

Due to the fast booming of micro electro mechanical systems, wireless sensor networking has been subject to extensive research efforts in recent years.

T.R. Yashavanth, (M.Tech) Computer Network & Engineering, "Jnana Sangama", Visvesvaraya Technological University, Belgaum, India.

Ravi S Malashetty, Department of PG Studies, "Jnana Sangama", Visvesvaraya Technological University, Belgaum, India.

C.R. Rashmi, (M.Tech) Computer Science & Engineering, CIT, Gubbi, Visvesvaraya Technological University, Belgaum, India.

It is well known as a general and ubiquitous approach for some applications like environmental and habitat monitoring, surveillance and tracking for military [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]. A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks.The cost of each sensor node is low but it contains required sensing, communicating and data processing components. Therefore, when a sensor node generates a report after being triggered by a special event, e.g., a surrounding temperature change, it will send the report to a data collection unit (also known as sink) through an established routing path [17].

Deployment of wireless sensor networks is usually done at adverse or unaccompanied environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and Sybil attacks [12], [18].

Further, injecting false data attack may affect wireless sensor networks [10].For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper-level error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report wrong wildfire location information to the sink, then expensive resources will be wasted by sending rescue workers to a no existing or wrong wildfire location. Therefore, it is crucial to filter the false data as accurately as possible in wireless sensor networks. At the same time, if all false data are flooding into the sink simultaneously, then not only huge energy will be wasted in the en-route nodes, but also heavy verification burdens will undoubtedly fall on the sink. As a result, the whole network could be paralyzed quickly. Therefore, filtering false data should also be executed as early as possible to mitigate the energy waste. To tackle this challenging issue, some false data filtering mechanisms have been developed [7], [8], [9], [10], [11], [12], [13]. Since most of these filtering mechanisms use the symmetric key technique, once a node is compromised, it is hard to identify the node.

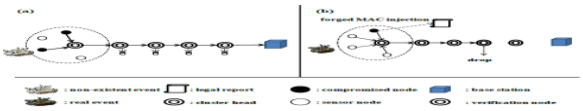

Fig1: False date injection and forged MAC attacks

2. Model and Design Goal

In this section, we formulate the network model, the security model, and identify the design goal.

2.1 Network Model

We consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes N = {N_0, N_1, . . .} randomly deployed at a certain interest region (CIR) with the area S. Sink is liable for initializing the sensor nodes and collecting data by these sensor nodes and sink is considered to be powerful and trustable data collection device, since it has enough storage and computational capabilities. In a location each sensor node $Ni \in N$ will be stationary. We assume that each sensor node has a unique nonzero identifier for differentiation purpose. In this case the communication will be bidirectional, i.e., two sensor nodes within their wireless transmission range (R) may communicate with each other. Therefore, if a sensor node is close to the sink, it can directly contact the sink. However, if a sensor node is far from the transmission range of the sink, it should resort to other nodes to establish a route and then communicate with the sink. Formally, such a wireless sensor network, as shown in Fig. 1, can be represented as an undirected graph G= {V, E}, where V ={v_1, v_2, . . .} is the set of all sensors N ={N_0,N_1, . . .} plus the sink, and $\varepsilon = \{(Vi, Vj)|Vi, Vj \in V\}$ is the set of edges. Let d (v_i, v_j) denote as the distance between v_i and v_j, then each e_{ij}, which indicates whether there exists a communication edge between two nodes v_i and v_j or not.

Let v_1 denote the sink. All sensor nodes $\frac{\gamma}{\{v_1\}} = \{v_2, v_3, \ldots\ldots\}$ can run the Dijkstra shortest path algorithm (see Appendix) to find their shortest paths to the sink v1, only if the graph $G = (V, \varepsilon)$ is fully connected.

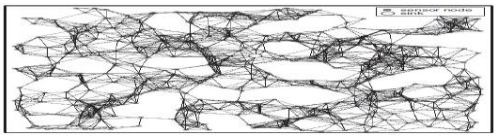

Fig 2: Wireless sensor network under consideration

Probability of fully connected $= (V, \varepsilon)$. Assume that the positions of these vertexes V = {v_1, v_2, . . .} are uniformly distributed in the area S with network density λ, where $\lambda = \frac{|v|}{S}$, and |V| denotes the cardinality of V. Based on the random graph theory, the probability that there are n nodes in an arbitrary region A with the area A is

$$P(N = n|A)$$
$$= \binom{|V|}{n}\binom{\pi.A}{|V|} pow\,(n).\left(-\frac{\pi.A}{|V|}\right) pow(|V| - n)$$
$$= \binom{|V|}{n}\left(\frac{A}{S}\right) pow(n).\left(1 - \frac{A}{S}\right) pow(|V| - n)$$

To calculate the full connection probability P_{con}, we first compute P_{iso}, the isolation probability of any node in G= {V, E}, where a node is called isolated if there exists no link among it and any other nodes. In other words, in some circle coverage with the area πR^2, except one node lies at the center, no other node exists. Suppose the border effects are neglected Fig. shows the full connection probability P_{iso} versus different transmission ranges R and |V|. It can be seen that the expected fully connected G= {V, E} can be achieved by choosing proper R and |V|.

2.2 Security Model

Since a wireless sensor network is unattended, a malicious adversary may readily launch some security attacks to degrade the network functionalities. In addition, due to the low-cost constraints, sensor nodes N ={N_0,N_1, . . .} are not provided with costly tamper-proof device and in an unprotected wireless sensor network it can easily compromised. Therefore, in our security model, we assume an adversary A can compromise a fraction of sensor nodes and obtain their stored keying materials. Then, after being controlled and reprogrammed by the adversary A, these compromised sensor nodes can collude to launch some injected false data attacks.

2.3 Design Goal

The design goal is to develop an efficient cooperative bandwidth-efficient authentication scheme for filtering the injected false data. The two desirable objectives are as follows.

2.3.1 Premature detection of injected false data by En-Route Sensor Nodes

The sink is said to be trustable and powerful data collection device. Undoubtedly, the sink will become a bottleneck if authentication is done at sink. Sink will also suffer from Denial of Service (DoS) attack if more injected false data comes into it. Therefore, it is critical to share the authentication tasks with the en-route sensor nodes such that the injected false data can be detected and discarded early. If injected false data is detected at the earliest, then large energy will be saved in the entire network.

2.3.2AchievingBandwidth-EfficientAuthentication

A bandwidth efficient authentication method has to be designed because costs of sensor node are low and energy constraint.

3. Proposed BECAN Scheme

We propose BECAN method in wireless sensor networks for filtering injected false data. Before proceeding to the BECAN scheme, the design rationale is introduced.

3.1 Design Rationale

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor x router (CNR)-based filtering mechanism.

Fig 3: Cooperative CNR based Authentication

As shown in Fig. in the CNR-based mechanism, when a source node N_0 is ready to send a report m to the sink via an established routing path R_{No}: $[R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_t \rightarrow Sink]$ it first resorts to its k neighboring nodes N_{N0} : $\{N_1, N_2, \ldots, N_k\}$ to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N_0 U N_{N0} to the sink via routing R_{N0} , where each mac_{ij}, $0 \leq i \leq k$, $1 \leq j \leq l$, represents N_i's MAC on m for R_j's authentication, and each mac_{is} represents N_i's MAC on m for the sink's authentication. As indicated in network model, the sink initializes all sensor nodes, and then each sensor node shares its private key with the sink. At the same time, according to the TinyECC-based non-interactive key pair establishment [19], the full bipartite key graph between N_0 U N_{N0} and R_{N0} can be established, as shown in Fig. 4. MAC design is reasonable because of the presence of full bipartite key graph. If there exist one uncompromised neighboring node which is participating in the reporting at the time of sending a false data to the sink by a compromised sensor node then the false data can be filtered. To achieve the bandwidth-efficient authentication, each mac_{ij} is set as one bit and each mac_{is} is α bit by using the above MAC in ZZ2 $\mathbb{Z}_{2^n}$ n technique. Then, the scale of MAC is only (l+ α) x (k + 1) bits.

3.2 Description of BECAN Authentication

The BECAN authentication scheme consists of two phases: sensor nodes initialization and deployment, and sensed results reporting protocol.

3.2.1 Sensor Nodes Initialization and Deployment

Given the security parameter k, the sink first chooses an elliptic curve defined over IF_p, where p is a large prime and function is a base point of prime order q with |q|=k. A secure cryptographic hash function h ( ) is then selected by sink, where h: {0, 1}*. Finally, the sink sets the public parameters as params = {E(IFp),G, q, h( )}. To initialize sensor nodes N_{N0} : $\{N_1, N_2, \ldots, N_k\}$, the sink invokes the Algorithm 1. Then, the sink deploys these initialized sensor nodes at a CIR in various ways, such as by air or by land. Even a rich literature in wireless sensor node deployment is provided [26], [27], we do not address the deployment in detail. After the deployment process we assume that uniform distribution of sensor nodes in CIR is done without loss of generality. Sensor nodes adjust or establish their routing cooperatively to the sink by considering shortest or a path adapted by some resource constraints with few available routing protocol when they are not occupied by reporting node. Speeding up of reporting is established by routing path.

3.2.2 En-Routing Filtering

When each sensor node R_i, $(1 \leq i \leq l)$, along the routing RN0 receives (m, T, MAC) from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the message (m, T, MAC) will be discarded. If the returned value is "accept," R_i will forward the message (m, T, MAC) to its downstream node, Otherwise, (m, T, MAC) will be discarded.

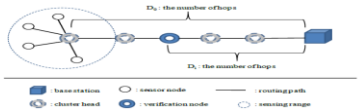

Fig 4: Selection of the verification nodes.

3.2.3 Sink Verification

If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys k_{is} of N_i, $0 \leq i \leq k$.

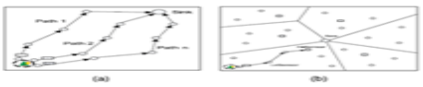

Fig 5: Reliability and Scalability

Reliability of the BECAN scheme. In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability.

Let FNR be the false negative rate on the true reports and tested as

$$FNR = \frac{number\ of\ true\ data\ that\ cannot\ reach\ the\ sink}{total\ number\ of\ ture\ data}$$

If FNR is small, the BECAN scheme is demonstrated high reliability. FNR can be increased by selectively dropping true report attack [18]. However, its adverse impact can affect any routing algorithm. Thus, for fairness, we only consider FNR that caused by 1) the number of uncompromised neighboring sensor nodes being less than k, 2) Some compromised sensor nodes polluting the true report. Fig. 10 shows the false negative rate FNR versus different number of reports. It can be seen, when the number of independent reports increases, the FNR decreases. Especially, when the number is five, the FNR is less than 10 percent. More independent entities report the event when an actual wildfire event happens. Thus, the multi-reports technology in BECAN scheme fits to the realistic scenarios. Hence BECAN method achieves good reliability.

4. Performance Evaluation

Energy saving is always crucial for the lifetime of wireless sensor networks. In this section, the performance of the proposed BECAN scheme is evaluated in terms of energy efficiency.

4.1 Energy Consumption in Non-interactive Key-pair Establishments

The proposed BECAN method has added computational cost because of expensive ECDH operations at the time of establishment of non-interactive key pair. Fortunately, since the non-interactive key pair establishments are averagely distributed in each sensor node and

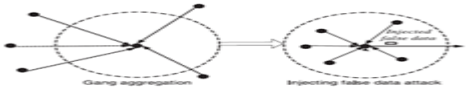

Fig 6: Gang Injecting

only executed once during the routing establishment, the ECDH operation is not a heavy burden. In order to achieve same amount of security as 1024 bit RSA, we can consider 160 bit elliptic curve during the design of TinyECC based sensor node [25]. Assume that, each sensor node is equipped with a low-power high performance sensor platform, i.e., MICAz [21]. Then, according to [19], this type of sensor platform only requires 50.82 mJ to establish a non-interactive shared key.

4.2 Energy Consumption in Transmission

The majority of injected false data can be filtered by BECAN within 15 hops during transmission. Thus, BECAN can greatly save the energy of sensor nodes along the routing path. In order to quantitatively measure the energy saving in BECAN, we compare the energy consumption of BECAN with that of SEF within the length of routing path H = 15 hops. For fair comparison, we set the parameter k = 4, and 0, three among four neighboring nodes colluding with the compromised source node N0, which corresponds to Nc = 1, 4 with T = 5 in SEF [9]. Because SEF does not consider the compromise of enrooting nodes, we also set $\rho = 0$ in BECAN.

5. Related Work

Recently, some research works on bandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in [9], [10], [11], [12], [13]. In [9], Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. Early verification of MACs correctness along the path when report is being forwarded is done at every node. Additionally sink will also verify MAC correctness which is carried in every report and it will reject false ones when injected false data is escaped from the en-routing filtering and is sent to the sink. In SEF, to verify the MACs, each node gets a random subset of the keys of size k from the global key pool of size N and production of MACs is done by using them. In order to reduce MAC size and to save bandwidth, bloom filter is adopted by SEF. Within 10 hops SEF can prevent 80-90 percent probability of injected false data by simulation. However, since n should not be large enough as described above, the filtering probability at each en-routing node $p = k(T-N_c)/N$ is relatively low. Besides, SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering. In [10], Zhu et al. present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the path, one is the lower association node, and the other is the upper association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses t + 1 individual MACs by XORing them to one. By analyses, only if less than t nodes are compromised, the sink can detect the injected false data. By creation of associations during the association discovery phase, the security method is contingent. Once the creation fails, the security

cannot be guaranteed. Further, as noted by Zhu et al.'s method in [7], similar as SEF, also adopts the symmetric keys from a key pool, which allows the compromised nodes to abuse these keys to generate false reports. Location-Based Resilient Secrecy (LBRS) is proposed by Yang et al. [11], reduces the damage caused during node compromise by adopting location key binding scheme and also in wireless sensor networks it mitigates the false data generation. More efficient location aware end-to-end security design (LEDS) to offer end-to-end security guarantee is proposed by Ren et al. in [12] which also includes assurance on high level data availability and an efficient way of en-routing false data filtering capability. Because LEDS is a symmetric key based solution, to achieve en-routing filtering, it requires location-aware key management, where each node should share at least one authentication key with one node in its upstream/downstream reportauth cell.

6. Conclusion and Future Work

In this paper, we have proposed a novel BECAN scheme for filtering the injected false data. By theoretical analysis and simulation evaluation, the BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi-reports. Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network [31]. In our future work, we will investigate how to prevent/mitigate the gang injecting false data attack from mobile compromised sensor nodes [32].

References

[1] Szewczyk, Robert, Alan Mainwaring, Joseph Polastre, John Anderson, and David Culler. "An analysis of a large scale habitat monitoring application." In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 214-226. ACM, 2004.

[2] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), 2002.

[3] Lu, Rongxing, Xiaodong Lin, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. "AICN: an efficient algorithm to identify compromised nodes in wireless sensor network." In Communications, 2008. ICC'08. pp. 1499-1504. IEEE, 2008.

[4] Lin, Xiaodong, Rongxing Lu, and Xuemin Sherman Shen. "MDPA: multidimensional privacy-preserving aggregation scheme for wireless sensor networks." Wireless Communications and Mobile Computing 10, no. 6 (2010): 843-856.

[5] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," Proc. IEEE GLOBECOM '09, Nov.-Dec. 2009.

[6] K. Ren, W. Lou, and Y. Zhang, "Multi-User Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[7] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[8] Zhu, Zhengjian, Qingping Tan, and Peidong Zhu. "An effective secure routing for false data injection attack in wireless sensor network." In Managing Next Generation Networks and Services, pp. 457-465. Springer, 2007.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM '04, Mar. 2004.

[10] Zhu, Sencun, Sanjeev Setia, Sushil Jajodia, and Peng Ning. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 259-271. IEEE, 2004.

[11] Yang, Hao, Fan Ye, Yuan Yuan, Songwu Lu, and William Arbaugh. "Toward resilient security in wireless sensor networks." In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 34-45, 2005.

[12] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. IEEE INFOCOM '06, Apr. 2006.

[13] Zhang, Yanchao, Wei Liu, Wenjing Lou, and Yuguang Fang. "Location-based compromise-tolerant security mechanisms for wireless sensor networks." Selected Areas in Communications, IEEE Journal on 24, no. 2 (2006): 247-260.

[14] Yu, Chia-Mu, Chun-Shien Lu, and Sy-Yen Kuo. "A dos-resilient en-route filtering scheme for sensor networks." In Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing, pp. 343-344, 2009.

[15] J. Chen, Q. Yu, Y. Zhang, H.-H. Chen, and Y. Sun, "Feedback Based Clock Synchronization in Wireless Sensor Networks: A Control Theoretic Approach," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2963-2973, June 2010.

[16] He, Shibo, Jiming Chen, Youxian Sun, David KY Yau, and Nung Kwan Yip. "On optimal information capture by energy-constrained mobile sensors." Vehicular Technology, IEEE Transactions on 59, no. 5 (2010): 2472-2484.

[17] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.
[18] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 8, no. 1, pp. 1-24, Jan. 2008.
[19] Liu, An, and Peng Ning. "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks." In Information Processing in Sensor Networks, 2008. IPSN'08. pp. 245-256. IEEE, 2008.
[20] Dong, Jingbo, Qing Chen, and Zhisheng Niu. "Random graph theory based connectivity analysis in wireless sensor networks with Rayleigh fading channels." In Communications, 2007. APCC 2007. Asia-Pacific Conference on, pp. 123-126. IEEE, 2007.
[21] MICAz: Wireless Measurement System, http://www.xbow.com/ Products/Product_ pdf _ files/Wireless_pdf/MICAz_Data sheet.pdf, 2010.
[22] Imote2: High-Performance Wireless Sensor Network Node, http://www.xbow .com / Products/Product_pdf _ files/Wireless_pdf/Imote2_Dat asheet.pdf, 2010.
[23] Boyd, Colin, Wenbo Mao, and Kenneth G. Paterson. "Key agreement using statically keyed authenticators." In Applied Cryptography and Network Security, pp. 248-262. Springer 2004.
[24] J. Black and P. Rogaway, "Cbc Macs for Arbitrary-Length Messages: the Three-Key Constructions," J. Cryptology, vol. 18, no. 2, pp. 111-131, 2.
[25] W. Mao, Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003.
[26] Li, Xu, Nicola Santoro, and Ivan Stojmenovic. "Localized distance-sensitive service discovery in wireless sensor and actor networks." Computers, IEEE Transactions on 58, no. 9,2009, 1275-1288.
[27] X. Li, A. Nayak, D. Simplot-Ryl, and I. Stojmenovic, "Sensor Placement in Sensor and Actuator Networks," Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication, Wiley, 2010.
[28] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," Ad Hoc Networks, vol. 5, pp. 24-34, Jan. 2007.
[29] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions," Proc. IEEE INFOCOM '99, pp. 708-716.
[30] Z. Benenson, C. Freiling, E. Hammerschmidt, S. Lucks, and L. Pimenidis, "Authenticated Query Flooding in Sensor Networks," Security and Privacy in Dynamic Environments, Springer, pp. 38-49, July 2006.
[31] Lin, Xiaodong, Rongxing Lu, Pin-Han Ho, Xuemin Shen, and Zhenfu Cao. "TUA: A novel compromise-resilient authentication architecture for wireless mesh networks." Wireless Communications, IEEE Transactions on 7, no. 4 (2008): 1389-1399.
[32] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An Efficient Identity- Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, Apr. 2008.

T.R. Yashavanth has received B.E (Computer Science & Engineering) degree from B G S Institute of Technology, Visvesvaraya Technological University, Karnataka, INDIA, with first class in 2009. Currently pursuing M.Tech (fourth sem) in Computer Networking & Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, INDIA. He has 03 years' experience in teaching. His areas of interest are Wireless Sensor Networks, MANET and Cloud Computing. He has 6 papers in National and 2 papers in International Conferences to his credit. He was a reviewer for the 8th IEEE Conference on Industrial Electronics and Applications (ICIEA 2013), which will be held in Melbourne, Australia during June 2013.

Prof. Ravi S Malashetty has received B.E (Computer Science & Engineering) degree from SLN Engineering College, Raichur, Visvesvaraya Technological University, Karnataka, INDIA, with first class in 2006. M.Tech in Computer Science & Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, INDIA. He has 03 years' experience in Industry and 1.5 years' experience in teaching. His areas of interest are Wireless Sensor Networks, MANET and Cloud Computing. He has 2 papers in International Conferences and 3 international Journals to his credit. He was a reviewer for ICIEA 2012 and also he was a session chair for IEEE Conference.

Rashmi C R has received B.E (Computer Science & Engineering) degree from Shridevi Institute of Engineering & Technology, Visvesvaraya Technological University, Karnataka, INDIA, with distinction in 2009. Currently pursuing M.Tech in Computer Science & Engineering from Channabasaveshwara Institute of Technology, Visvesvaraya Technological University, Karnataka, INDIA. She has 01 year experience in teaching. Her areas of interest are Image Processing, Signal Processing and Computer Networks. She has 01 paper in National level technical symposium to her credit.