A Vision of Hybrid Security Framework for Wireless Sensor Network

KEYWORDS WSN, MOTE, NS-2, Packet.

D. P. Mishra	Ramesh Kumar
Research Scholar, CSVTU, Bhilai	Professor in Computer Sc. & Engineering, BIT, Durg

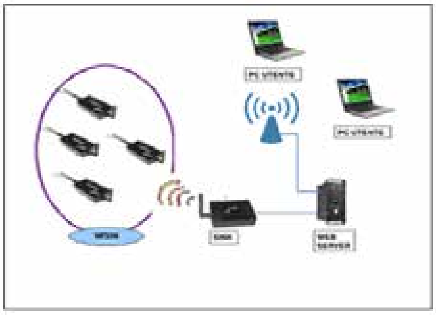
ABSTRACT *Sensor network is having large number small sensor nodes deployed in some geographical area for sensing different parameter as per the requirement. Purpose of the network is to sense different parameters and report the happenings of the respective area where the nodes were deployed in. Sensor networks are used in variety of applications. In military it is used for surveillance and target tracking. In industrial applications, sensor networks are used for monitoring hazardous chemicals. It is used for monitoring the environment and in early fire warning in forests as well as seismic data collections. Sensor networks face new challenges due to their peculiarities, primarily the stringent energy constraints to which sensing nodes are typically subjected which is not known in cellular and ad-hoc wireless networks. The unique features of sensor networks lead to affect the hardware design of the nodes at least four levels: power source, processor, communication hardware, and sensors. In this paper, we report on currents and new trends in sensor networks. We also present vision and future for wireless sensor networks.*

INTRODUCTION

Wireless Sensor Network (WSN) is a new technology foreseen to be used increasingly in the near future due to their data acquisition and data processing abilities. Security for WSNs is an area vulnerable to security breaches because they are physically more accessible to possible adversaries. The memory and energy limitations of sensor nodes are a major obstacle to implementing traditional security solutions. The fact that wireless sensor networks utilize unreliable communication network. These nodes, in order to snoop or sabotage, can carry out a variety of attacks against the network including sinkhole and wormhole attacks.

In sensor Network each node helps every other node in the network by forwarding their packets. If all is well attitude is exhibited by all participating nodes then really there is no issue. However, if these nodes operate in a physically insecure environment, they are vulnerable to capture and compromise with third party or man in middle attack by malicious node. In addition, the communication medium being wireless, restricts enforcement of rigorous node memberships, so a number of malicious nodes also participate in the network.

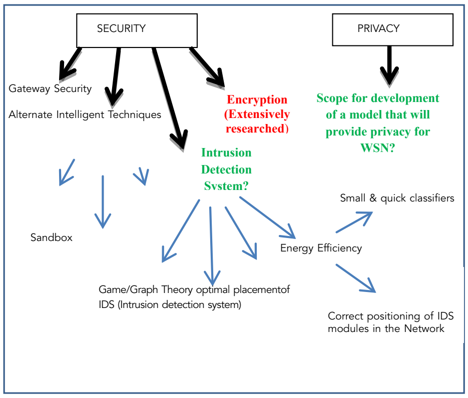
While all networks are subject to common threats, remote wireless sensor networks are additionally left unattended once deployed makes the provision of adequate security countermeasures even more difficult [22] has indicated that the future of sensor nodes would lie in driving the cost down rather than in increasing the memory or energy capabilities that needs to be considered in order to protect the functionality of these networks, the data they convey and the location of their members, [22]. The security models and protocols used in wired and other networks are not suited to WSNs because of their severe resource constraints. [14] WSNs consist of hundreds or thousands of low-power, low-cost nodes having a CPU, power source, radio, and other sensing elements. They have one or more points of centralized control called base stations or sink nodes and are responsible for taking readings from multiple sensor nodes and processing at aggregation points shown in Fgure-1.



Literature reviewd

Research in the area of Wireless Sensor Networks has increased exponentially since the turn of the millennium. Researchers are focused on addressing the myriad of challenges, that have spawned from the limited resource capabilities of the hardware i.e. memory, processing power, bandwidth and energy deposits. In particular, much research is currently being conducted in the following areas:

- Increasing network lifetime.
- Improving reliability of data transfer.
- Finding solutions to assist easy deployment and maintenance.
- Developing techniques that will enforce secure, private and trustworthy networks.


SECURITY
PRIVACY
Gateway Security
Alternate Intelligent Techniques
Encryption (Extensively researched)
Scope for development of a model that will provide privacy for WSN?
Intrusion Detection System?
Small & quick classifiers
Sandbox
Energy Efficiency
Game/Graph Theory optimal placementof IDS (Intrusion detection system)
Correct positioning of IDS modules in the Network

Literature survey, is attempt to present and evaluate the work that has been done on the subject of Security and Privacy for WSNs. Presently, there are two schools of thoughts that are being argued in this area; Figure-2 illustrate the scope of research.

Many researchers insist that WSNs will never become secure enough for commercial use, unless security and privacy measures are considered during the design phase. Such researchers are primarily interested in developing secure protocols from scratch. Others state that intelligent security add-ons may be more than sufficient, whilst requiring less development costs. Work from both sides is presented throughout this literature survey.

Encryption

Sensor Networks mainly operate in public or uncontrolled areas, over inherently insecure wireless channels. It is therefore trivial for a device to eavesdrop or even inject messages into the network. The traditional solution to this problem has been to espouse techniques such as message authentication codes, symmetric key encryption schemes and public key cryptography, [10] since wireless sensor motes are severely constrained, the major challenge here is to implement this encryption in an efficient way without sacrificing their strength.

Shared Keys

One method of protecting any network against outsider attacks is to apply a simple key infrastructure. However, it is known that global keys provide no network resilience and pairwise keys were not a scalable solution. A more intuitive solution is needed here for WSNs.[14] , TinySec was developed as a first attempt to introduce security to the link layer of the TinyOS suite. This was done by incorporating software-based symmetric keying with low overhead requirements. Unfortunately, not all vulnerabilities of TinySec have been addressed i.e. how to avoid insider attacks. In contrast, ZigBee or the 802.15.4 standard introduced hardware-based symmetric keying with success. Some researchers are investigating the possible use of public cryptography to create secure keys during network deployment and maintenance phases,[18].Extensive research is also being conducted on topics such as key storage and key distribution [5], key maintenance and shared key pools [9].

Secure Groups

Since sensor nodes are required to group themselves in order to fulfil a particular task, it is necessary that the group members communicate securing between each other, despite the fact that global security may also be in use. Unfortunately, secure grouping has not been intensively researched. Exceptions are the solutions where more powerful nodes are in charge of protecting the members of static groups. Such solutions would nicely compliment the dominance of cluster based protocols such as LEACH [11]

Figure-3: Mica Mote (Sensor Node)

Data Aggregation

In order to reduce overhead costs and network traffic, sensor nodes aggregate measurements before sending them to the base station. Such data is particularly enticing to an attacker. An adversary with control over an aggregating node, can choose to ignore reports or produce false reports, affecting the credibility of the generated data and hence the whole network.

The main aim in this area is to use resilient functions, that will be able to discover and report forged reports through demonstrating the authenticity of the data somehow. Wagner 2004[26] established a technique in which the aggregator uses Merkle hash trees to create proof of its neighbors' data, which in turn is used to verify the purity of the collected data to the base station. Another approach [7], takes advantage of the network density by using the aggregator's neighbor's as witnesses. It is also possible to reduce the amount of traffic heading to the base station by using bloom filters to filter out the false aggregations [17]. Improvements still need to be made in this area, such as minimizing the amount of negotiation data generated by interactive algorithms

Secure Protocols

The main challenge in this area of research is to discover new protection techniques that can be applied to existing routing protocols, without forfeiting connectivity, coverage or scalability. Perrig et al 2004 made the first attempt to design secure protocols for sensor networks. This protocol also known as SPINS: (Security protocols in Sensor Networks) provides data authentication, replay protection, semantic security and low overhead. This work has in turn been used to secure cluster based protocols such as LEACH Ferreira et. al. 2005, Karlof and Wagner [14] have provided an extensive analysis on the routing vulnerabilities of WSNs and possible countermeasures. According to their study, common sensor network protocols are vulnerable due to their simplicity and hence security should be built into these protocols during design time. In particular, their study targets TinyOs beaconing, directed diffusion and geographic routing. The attacks they focus is still theoretical and still not been implemented practically on any type of hardware. This research has been supported by Mun and Shin 2005, who suggest countermeasures for routing attacks that establish trust relationships between nodes and authenticate sent packets whilst checking node bi-directionality. Other researchers have focused on developing techniques that target specific attacks such as DoS,[18]. In contrast moved away from routing information and looked at the application layer in order to detect and correct aberrant node behavior.

Privacy

Sensor Networks are systems that rely on the collection of information to perform their tasks. Therefore, an additional system requirement is that guidelines regarding fair information practices are built into the networks, in an attempt to protect privacy rights. To elaborate, content, identity and location privacy of the network need to remain intact for a system to be considered 'private'. The literature suggests that solutions such as data encryption, access control, the anonymous storing of data and distributed query processing might be the way to go. Olariu et al 2005 [21] take a good stand at privacy issues by defining schemes that maintain the anonymity of the virtual infrastructure of WSNs. This area still remains vastly unexplored. Scenarios need to be explored where privacy is being exploited and solutions need to be devised to solve these issues.

Other Issues

Due to the immaturity of sensor networks as a networking solution, there is a plethora of security applications that have not yet been fully investigated. Such an example is the use of mobile agents, which are a powerful tool for collaborative processing. It is therefore crucial that a network is able to identify and authenticate these agents and the instructions they deliver to the network, else it would be very easy to inject false information into the nodes or modify collected results.

Open Research Areas

Research in the field of WSNs is growing rapidly and achieving tangible results that apply to real life scenarios. However, this field is still at its infancy and there is much room for improvement. Public key cryptography, intrusion detection and reaction are fairly new areas. Secure data aggregation algorithms need to be optimized and secure routing algorithms need to comply with the coverage, connectivity and fault tolerance requirements of the networks, also privacy of information flow needs to be addressed. To

Summarized, research attention needs to be directed to the following

- **Tolerating the lack of physical security**
- **Optimizing the security infrastructure in terms of resources (energy and computation)**
- **Detecting and reacting to DoS attacks**
- **Raising the issue of social privacy problems**
- **Management and protection of mobile nodes and base stations.**
- **Secure administration of multiple base stations with delegations of privileges.**

MAJOR CONTRIBUTIONS

The Hybrid Intrusion Detection System

Karloff and Wagner 2003[14] specified the security goals for WSNs that the research community should be aiming for. They state that ideally, one would require a security solution that guarantees the integrity, authenticity and availability of all messages even in the presence of attackers, no matter what their power. In the presence of outsider attackers these idealized goals may actually be achievable. However in the presence of insider attackers, especially ones with laptop capabilities, these goals need to be reassessed.

Attack Replication/Verification

In order to perform misuse detection it is necessary to have signatures of the attacks on the network. Given this database of signatures, IDS can match data packets occurring on the network to those of malicious nature, hence setting alarms in the network. Even anomaly detection techniques require some knowledge of malicious data in order to determine which features of data are more likely to be useful for classification purposes. [14] have identified a number of attacks that can be launched on the routing layer of sensor networks. They agree that WSNs are vulnerable to the following DoS attacks to layer 3 of the protocol stack:

- Spoofed altered or replayed data
- Selective forwarding Sinkhole attacks
- Sybil attack
- Hello flood attacks
- Wormholes
- Black hole
- Acknowledgement spoofing

Many researchers proposed several methods for obtaining energy efficiency and secrecy. However, the contributed methods are not giving the intended outcome as they are prone to security attack. Summary of noteworthy contribution in the field of proposed work is as under

- Security issues are similar (MANET vs. WSNs) but not the defense mechanisms
- Public-key cryptography is expensive for WSNs
- WSNs must rely on private-key cryptography
- Symmetric-key cryptography based on SR or DV is not suitable for WSNs
- Punishing, reporting selfish or misbehaving nodes is a promising work
- SNEP and μTESLA are security protocols optimized for WSNs

METHODOLOGY

We propose the use physical hardware and simulations to obtain data test all developed techniques and prove their suitability to real sensor network applications. Figure-3 shows sensor node used for gathering different parameters

For replicating DoS attacks on sensor network hardware, the following problems need to be addressed.

Data Extraction

Using regular motes to intercept all communications in its transmission range. The data they hear can then be relayed back to a computer via a serial cable for logging. In order to do this however, it is necessary to modify the node's code, so that it operates as an eavesdropper and not as a network member. This solution is likely to be the most simple to implement.

Using a commercial wireless sniffer. This can be attached to a wireless laptop that can intercept the communications at different points of the network

This method however isn't as favored as the previous method as much effort will be associated with configuring the wireless receiver of the laptop to the specifications of the wireless chips in the nodes

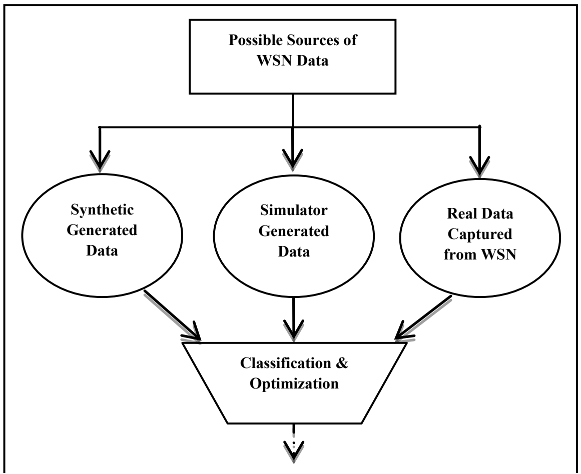

Possible Sources of WSN Data
Synthetic Generated Data
Simulator Generated Data
Real Data Captured from WSN
Classification & Optimization

Figure 4: Possible Sources of WSN Data

Figure 4: Shows how data can be generated for the research work. Ideally we would like to extract data from

working WSN; however simulated model and synthetic data can be used to generate data from which further research can be pursued

Attack
Malicious activity can be replicated by using a laptop with a modified wireless card and running the same protocol stack as the network. Initially it would be simpler for attacker to be a regular sensor node running malicious code. A simple initial attack may be to change the frequency with which the malfunctioning node forwards messages, in an attempt to flood the network. More complex attacks will need to be replicated by modifying protocol specific parameters. A contingency plan here would be to generate such attack data synthetically based on known signature analysis techniques common to those used in the internet.

Classification
This part of the research has to do with developing and testing the fault tolerant and energy efficient model that we are proposing. To follow is an outline of the proposed methodology which will make this feasible.

Signature Generation
Both anomaly detection and misuse detection techniques will be trailed to find the most accurate solution for the hybrid IDS. For the misuse detection part, signatures will be generated automatically using a honeypot like system, as this would be a more efficient solution than wasting time analyzing audit data in an attempt to generate attack signatures. It is proposed that the sensor network in its entirety be considered as a honeypot. In particular, a laptop or individual node attacks the network. Specific points in the network relay information back to a computer which will then use string matching techniques, similar to those proposed in [5]

Classifiers & optimization
We are considering trailing a variation of classifiers on the attack and normal data collected from the network. We will be looking at clustering methods such as K-means nearest neighbor's and self-organizing maps. Also we will be testing Support Vector Machine methods, Artificial Neural networks and Markov Models. We will require data sets that contain normal network activity and malicious activity of some sort. These sets will be the training sets for the classifiers. After the classifiers have been trained to identify the difference between the 2 classes accurately we will test them on a data set they have never seen before. After the preliminary performance results are gathered, attention will be spent on optimizing the best classifier such that its resource demands on the network are minimized. This will possibly involve mathematically remodeling the classifier such that the amount of memory and processing power it requires are reduced to a minimum. The goal at this stage is to introduce further improvements to network longevity, especially in the presence of attacks. Online testing and simulation will help to determine the changes if any to network lifetime. Optimization and testing stages will need to be interleaved recursively to ensure the best results.

Optimal Placement
In an attempt to further optimize the system, we will be considering how to optimally place the intrusion detection modules around the network. In particular one would need to determine the exact number of agents that are necessary to monitor all possible packets flowing through the network and also which nodes in the network need to be equipped with this agent in order to do this Anjum et al 2004 [2]. This is where graph and game theory techniques will point out the best locations to place the intrusion detection agents in the network. Nodes with agents will obviously have their energy sources drained faster than those that don't, so schemes for repositioning the agents on nodes with more power need to be considered. In clustering protocols such as LEACH [11], the agents may be placed on all or some of the cluster heads, since the protocol demands that these nodes have higher energy stores than the cluster members. Determining the single weakest point of network to apply the agent to via game theory should also provide interesting outcomes. Mobile code application may need to be considered in this part of the research. The difference optimal placement make on network lifetime will be determined once again via online testing.

Recovery
One thing that many researchers don't consider is what to do when an attack has been identified by a high accuracy classifier. In this stage of research we will be considering and testing recovery techniques for the replicated routing attacks. One possible method may include purging the malicious node by making legitimate nodes remove the attacker from their routing tables. Another possibility is sending the entire network to sleep for a pre-agreed amount of time, in which way to conserve energy whilst the network is under attack. In an attempt to generate a hybrid security solution such techniques must be included. This will also prove to be one of the most complex parts of the research

Benchmarking
In an attempt to evaluate the overall performance of the developed system, an in depth comparative study will need to be conducted against other security mechanisms for WSNs. In particular, we will be looking at how our hybrid system competes with encrypting protocols which use key pools and other intrusion detection systems that may have fronted in the area by then. A trial against the secure protocol Tiny Sec is a must. [24]. other protocols such as S-LEACH and S-MAC are also on the agenda. Comparative measures that we will be considering include detection accuracy, false positive alarms, energy consumption and most importantly network lifetime under attack over network lifetime without attacks

Resource requirement for research work
A basic sensor network of 30 motes initially, 5 motes will be sufficient for the preliminary research. Additional sensors may need to be attached to the motes to enrich the application being tested. An average PC with serial and parallel port capabilities that will act as the gateway between the WSN and the user. This PC will be used to log data coming off the network and also for analysis of data and the development of classifiers. A laptop with wireless network capabilities that will simulate laptop class attacks on the network. Software for classifier development including C compilers, SQL database & MATLAB. NS-2 or OPNET or TOSSIM for simulation.

CONCLUSIONS

Proposed framework for fault tolerant and energy efficient intrusion detection in wireless sensor networks will provide desired security solution for real-life sensor network hardware and address the following.

- Provide protection against outsider attacks, on the ba sic of intrusion detection system that offers protection against malicious insider attacks.

- Extends the lifetime of a network under attack for as long as possible. Hence looking at finding an energy efficient and accurate classifier to take on the job of detecting malicious activity on the network.
- Make the use of game theory strategies in combination with graph theory principles to determine the most effective points in the network to place these intrusion detection agents.
- Hybrid framework will also incorporate recovery techniques that will help the system recover and overcome launched attacks.
- Final system to be applied successfully to both applications with high volumes of malicious activity and also applications where malicious activity is negligible.

REFERENCE

[1] Agah A., Das S. K., Basu K. and Asadi M. 2004, Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach, in Proceedings - Third IEEE International Symposium on Network Computing and Applications, NCA 2004, Aug 30- Sep 1 2004, Proceedings - Third IEEE International Symposium on Network Computing and Applications, NCA 2004, (Cambridge, MA, United States), 343– 346, IEEE Computer Society, Los Alamitos, CA 90720-1314, United States. | [2] Anjum F., Subhadrabandhu D., Sarkar S, and Shetty R. 2004, On Optimal Placement of Intrusion Detection Modules in Sensor Networks, in Proceedings - First International Conference on Broadband Networks, BroadNets 2004, Oct 25-29 2004, Proceedings - First International Conference on Broadband Networks, BroadNets 2004, (San Jose, CA, United States): 690–699, IEEE Computer Society, Los Alamitos, CA 90720-1314, United States, 2004. | [3] Avancha S., Undercoffer J., Joshi A., and Pinkston I. 2003, Secure Sensor Networks for Perimeter Protection, Computer Networks Wireless Sensor Networks, 43(4): 421–435 | [4] Brutch P. and Ko C. 2003, Challenges in Intrusion Detection for Wireless ad-hoc Networks, in Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on: 368–373. | [5] Chan H., Perrig A., and Song D. 2003. Random Key Predistribution Schemes for Sensor Networks," in Security and Privacy Symposium, 2003. :197–213. | [6] Doumit S. S. and Agrawal D. P. 2003, Self-Organized Criticality and Stochastic Learning Based Intrusion Detection System for Wireless Sensor Networks, in MILCOM 2003 - 2003 IEEE Military Communications Conference, Oct 13-16 2003, vol. 1 of Proceedings - IEEE Military Communications Conference MILCOM, (Monterey, CA, United States) : 609–614, Institute of Electrical and Electronics Engineers Inc., Piscataway, United States | [7] Du W., Han Y. S., Deng J., and Varshney P. K., 2003. A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks. Proceedings of the ACM Conference on Computer and Communications Security :42 – 51 | [8] Du. W., Deng J., Hans Y., Chen S. and Varshney P. 2004. A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge in INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, (1):597. | [9] Eschenauer L. and Gligor V. D.,2002. A Key-Management Scheme for Distributed Sensor Networks in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA: ACM Press:44-47 | [10] Ferreira A. C., Vilaca M. A. , Oliveira L. B., Habib E. , Wong H. C. , and Loureiro A. A. 2005, On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks, in Networking - ICN 2005, Apr 17-21 2005, 3420 of Lecture Notes in Computer Science, (Reunion Island, France), 449–458, Springer Verlag, Heidelberg, D-69121, Germany. | [11] Hsin C.-F. and Liu M.,2002. A Distributed Monitoring Mechanism for Wireless Sensor Networks, in Proceedings of the 2002 ACM Workshop on Wireless Security, Sep 28 2002, Proceedings of the Workshop on Wireless Security, (Atlanta, GA, United States) : 57–66, Association for Computing Machinery. | [12] Intanagowiwat C., Govindan R., and Estrin D. 2000. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks : 56–67. | [13] Kaplantzis S.,October 2004. Classification Techniques For Network Intrusion Detection. tech. rep., Monash University, ECSE, | [14] Karlof C., Sastry N., and Wagner D. Nov 3-5 2004. Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks in SenSys'04 - Proceedings of the Second International Conference on Embedded Networked Sensor Systems:162–175, 2004. | [15] Kodialam M.and Lakshman T. 2003. Detecting Network Intrusions via Sampling: A Game Theoretic Approach, in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, vol. 3:1880–1889. | [16] Kreibich C. and Crowcroft J. 2004, Honeycomb: Creating Intrusion Detection Signatures using Honeypots, SIGCOMM Comput. Commun. Rev., 32(1): 51–56. | [17] L. Li and J. Halpern,June 2001. Minimum- energy module wireless networks revisited. | [18] Malan D., Welsh M., and Smith M. 2004, A Public-Key Infrastructure for Key Distribution in tinyos Based on Elliptic Curve Cryptography, in Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference : 71–80. | [19] Muruganathan S. D., Ma D. C., Bhasin R. I., and Fapojuwo A. O. , 2005 A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks IEEE Communications Magazine, 43(3): 8–13. | [20] Newsome J., Shi E., Song D., and Perrig A. 2004, The Sybil Attack in Sensor Networks: Analysis and Defenses, in Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, Apr 26-27 2004, Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, (Berkeley, CA., United States):259–268, Association for Computing Machinery, New York, United States. | [21] Olariu S., Xu Q., Eltoweissy M., Wadaa A., and Zomaya A. Y. 2005, Protecting the Communication Structure in Sensor Networks, International Jounral of Distribted Sensor Networks, 1:187–203. | [22] Perrig A., Stankovic J. and Wagner D. 2004, Security in Wireless Sensor Networks, Communications of the ACM, 47 (6): 53–57. | [23] Roman R. , Zhou J. and Lopez J , 2005,. On the Security of Wireless Sensor Networks: International Conference on Computational Science and Its Applications vol. 3482 of Lecture Notes in Computer Science, (Singapore): 681–690. | [24] Sastry N. and Wagner D.2004. Security Considerations for IEEE 802.15.4 Networks - Proceedings of the 2004 ACM workshop on Wireless security, Philadelphia, PA, USA: ACM Press:2-42 | [25] Seshadri A. , Perrig A. , Van Doom L., and Khosla P. 2004, Swatt: Software-Based Attestation for Embedded Devices- in Proceedings - 2004 IEEE Symposium on Security and Privacy, May 9-12 2004,Proceedings - IEEE Symposium on Security and Privacy, (Berkeley, CA, United States), 272–282, IEEE Computer Society, Los Alamitos;Massey University, Palmerston, United States;New Zealand. | [26] Wagner D. 2004, Resilient Aggregation in Sensor Networks SASN'04 – Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks:78 – 87, 2004. Data aggregation;Sensor networks;Node capture attacks;Multi-party computation;Robust statistics;Average;Mean;Median;. |