Research Paper

Volume : 5 | Issue : 1 | JANUARY 2016 • ISSN No 2277 - 8179

A Game Theory Based Injected False Data Filter for Wsn

Medical Science

KEYWORDS : Wireless sensor network, injecting False Data attack, cooperative bit-compressed authentication etc.

Veena Jain Department of CSE/IT, Abha Gaikwad-Patil College of Engineering, Nagpur

Prof. Gajanan Patle Department of CSE/IT, Abha Gaikwad-Patil College of Engineering, Nagpur

ABSTRACT

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Sensor nodes are essentially small computers with extremely basic functionality. They consist of a processing unit with limited computational power and a limited memory, one or more sensors, a radio communication device and a power source. Power consumption is an important issue for the network to be self-sustainable. Minimizing the cost of deployment is of paramount importance. Since WSN is a nascent technology, many of the existing general purposes solutions in the market are expensive and/or they are not well tailored for use in the developing world. In a large WSN, In-network data aggregation (i.e., combining partial results at intermediate nodes during message routing) significantly reduces the amount of communication overhead and energy consumption. False Data injection is another serious threat in wireless sensor networks. Injecting false data attack is the one in which opponent reports fake information to sink that will create a error at top and energy waste in en-route nodes. To detect and filter the false data injection in the early stage, BECAN (Bandwidth Efficient Co-Operative Authentication Scheme for Filtering Injected False Data in Network) Scheme is used. Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios. It can save energy by early detecting and filtering the majority of injected false data using cooperative bit-compressed authentication technique and random graph generation.

INTRODUCTION

In recent years, cyber attacks have been growing increasingly sophisticated, with attacks designed to exploit the psychological, social, financial vulnerabilities of targeted users / organizations / institutions to defraud them or infect their system with viruses or garbage data. These kinds of attacks are often difficult to distinguish from ordinary network access, and are difficult to detect using conventional filters, decrypting techniques and firewalls. Under these circumstances, it is all the more important to be able to quickly identify data attacks and develop protective security measures tailored to the requirements of WSN.

Many defensive techniques are designed to protect program control flow integrity. Although earlier work did suggest the existence of attacks that do not alter control flow, such attacks are generally believed to be rare against real-world software. On the other hand non-control-data attacks are futuristic and realistic. We can demonstrate that many real-world applications are vulnerable to such attacks. In each case, the generated attack results in a security compromise equivalent to that due to the control-data attack exploiting the same security bug. Non-control-data attacks corrupt a variety of application data including configuration data, user input data, and decision-making data. The success of these attacks and the variety of applications and target data suggest that potential attack patterns are diverse. Attackers are currently focused on control-data attacks, but it is clear that when control flow protection techniques shut them down, they have incentives to study and employ non-control-data attacks. In today's era of IOT (Internet of Things),the other important parameter in developing the protection tool against data attack is the type of network under consideration. Here in this paper, we are focusing on data attacks in Wireless Sensor Networks (WSN).

A wireless sensor networks (WSN), or better a mesh WSN, usually consists of one sink (or base station) able to manage all the communications between other nodes. This kind of network has fixed routes, excepting when there are nodes' failures. Thus, the base station (or, again, router if the WSN works up to the network level rather than link level) determines and optimizes the paths of communication in the network. Instances of WSNs are networks monitoring a bridge, the temperature in several parts of a city (although this case is more complex due to the big area to monitor) or an ancient monument.

A mobile ad-hoc network (MANET) even is a WSN if its scope is that of sensing the environment around the network. However, the words "mobile" and "ad-hoc" are often used to refer to all those networks consisting of nodes continuously moving in any direction (for this reason the word mobile). Consequently, this kind of network must repeatedly reconfigure its routes. All this work is done by every node in the network since MANET doesn't have a fixed central controller (for this reasons the word ad-hoc). Furthermore, this kind of networks usually uses different devices with respect to other WSNs because the management of energy and communications is totally different. Examples of MANETs are networks formed by devices installed within cars (VANET) to monitor accidents, traffic and so on, or a network consisting of drones.

The false data injection which can be done at any stage, results in information loss as well as energy loss. The sink helps in identifying false data to be filter out before sending to destination ,this create the bottle neck at sink results in Denial of service attack. The Bandwidth efficient cooperative association scheme can be used to effectively filter out false data in the network. In our proposed project, data are securely aggregated at one node and verification process done at end nodes to reduce the burden at sink. The secure aggregation at en route node and detection of false data is done at same point result in reducing bottle neck at sink, high reliability, and efficient energy saving in wireless sensor network.

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, Wormholes, and Sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack. 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 nonex-

istent or wrong wildfire location.

In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability. The main contributions of this paper are threefold.

- First we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication.
- Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient ;and
- Third, we develop a custom Java simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

Random graph characteristics of wireless sensor node

As mentioned in first point of our proposed plan, it is necessary to continuously and closely monitor the entire network for stable connectivity. Data attacks directly hamper the connectivity model of WSN. Any loss of connectivity can be an alarming condition for possible data attack. Connectivity is an essential merit of wireless sensor networks. There has been great interest in exploring the minimum density of sensor nodes that is needed to achieve a connected wireless network. The connectivity is lost or compromised when WSN are breached for externally forced data attacks. For controlled data attack, it is necessary for an advisory to compromise the node for alterations in data packets. This may result in temporary isolation of a node from network. Our one of the aim is to detect such short time isolated nodes and focus on them for possible tampering in data packets. Moreover, the numerical result shows that the fading effect would degrade the connectivity of the wireless sensor networks.

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. 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 uses them to producing the MACs. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. By simulation, SEF can prevent the injecting false data attack with 80-90 percent probability within 10 hops. SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering. 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. However, the security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed.

Filtering of maliciously injected data

Once we are able to detect trouble nodes or zones in the network, we can apply different filtering algorithms to test and filter unwanted data. Instead of putting all burdens on sink node for data filtering, we are proposing to distribute the filtering load on complete WSN. The distributed approach will definitely improve the response time and overall efficiency of network.

In a large-scale sensor network individual sensors are subject to security compromises. A compromised node can inject into the network large quantities of bogus sensing reports which, if undetected, would be forwarded to the data collection point (i.e. the sink). Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network.

IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Algorithm CNR Based MAC Generation

1: **procedure** CNRBASEDMACGENERATION
Input: $params$, $N_i \in (N_{N_0} \cup N_0)$, m, T, R_{N_0}
Output: Row_i
2: N_i uses the non-interactive keypair establishment to compute shared keys with each node in $R_{N_0} : [R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow Sink]$ as $k_{i1}, k_{i2}, \cdots, k_{il}, k_{is}$, where k_{is} is N_i's private key distributed by the *sink*
3: **if** N_i believes the report m is true **then** ▷ a neighboring node is assumed having the same ability to detect a true event as the source node and correctly judge the report m.

Modules

BECAN Scheme

A novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability.

- •) First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication;
- •) Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; and
- •) Third, we develop a custom simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

Early detecting the injected false data by the en-route sensor nodes

The *sink* is a powerful data collection device. Nevertheless, if all authentication tasks are fulfilled at the *sink*, it is undoubted that the *sink* becomes a bottleneck. At the same time, if too many injected false data flood into the *sink*, the *sink* will surly suffer from the Denial of Service (DoS) attack. 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. The earlier the injected false data are detected, the more energy can be saved in the whole network.

Volume : 5 | Issue : 1 | JANUARY 2016 • ISSN No 2277 - 8179

Gang Injecting False Data Attack

We introduce a new stronger injecting false data attack, called gang injecting false data attack, in wireless sensor networks. This kind of attack is usually launched by a gang of compromised sensor nodes controlled and moved by an adversary *A*. As shown in Fig. 2, when a compromised source node is ready to send a false data, several compromised nodes will first move and aggregate at the source node, and then collude to inject the false data. Because of the mobility, the gang injecting false data attack is more challenging and hard to resist.

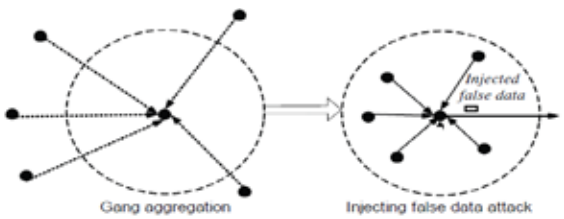

Fig2. Gang Injecting False Data Attack

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

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

If FNR is small, the BECAN scheme is demonstrated high reliability.

Simulator

Wireless sensor networks face many problems that do not arise in other types of networks: Power constraints, limited hardware, decreased reliability, and a typically higher density and number of nodes than those found in conventional networks are few of the problems that have to be considered when developing a simulation tool for use in wireless sensor networks. Hence, most of network simulators fail to support all the following criteria: easy, where the vast amount of variables involved in the definition of a WSN experiment requires the use of specific input scripting languages, with high-level semantics, extendable where simulation is used to test novel techniques in realistic and controlled scenarios (researchers are usually interested in comparing the performance of a new technique against existing proposals) and scalable where increasing number of nodes without degrading the performance of network, so a simulation tool for WSNs localization is required specifically for the analysis of different types of localization schemes.

The proposed simulation tool has the following advantages:

- Supports completely large scale networks (scalable simulator).
- All simulator classes are packed into a referenced DLL file for better modularity design. For example, various localization algorithms can be implemented by encapsulating each one into a separate DLL file.
- Developers can write their own localization algorithm into a DLL file and reference it to the proposed simulation tool (extendable simulator).

The proposed simulation tool is a discrete event simulator which is written in the Java programming language. This discrete event simulation tool operates on the basis of chronological consecutive events to change a system's state. These events are processed by the simulation kernel. User-defined localization algorithms are implemented as Java classes and mostly utilize simulation tool concepts. Node composition and network layout along with environmental and setup parameters are set via user interface. The modules are compiled and linked with the simulation kernel, and result in the simulation application.

The simulation tool architecture design is flexible, and modular, allowing for customizations to be made using an object oriented component files. Such an approach allows for users to adapt the simulation tool, or extend it to different localization algorithms.

The proposed simulator has following features

- Supports two ray ground and shadowing propagation models.
- All events done during simulation time are written into an external trace file.
- Supports Wormhole, Sybil, Spoofing and Replay attacks and their defense algorithms.
- Supports multiple type of sensor modes like MICA2 and TelosB

CONCLUSION

In proposed system, we are using BECAN Scheme for filtering false data using CNR based Mac generation techniques. It also helps in achieving high en routing filtering probability and high reliability by reducing bottleneck at sink. We make use of en-route filtering detection and filtering algorithm, which keep visiting the suspicious nodes to detect any abnormality in data packets or possibility of data attack. Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios.

REFERENCE

[1] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014. | [2] V.Chitra, L.Hameetha Begum, M.Ramya, R.Udhaya," Filtering False Data Injection | Using Becan Scheme in Wireless Sensor Networks", IJREAT International Journal of | Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014. | [3] Amuthan Mathy.P, Gowri Sankar.U, "Filtering Injected False Data in Wireless Sensor | Networks by Using L, F, S Nodes and Key Distribution", International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014. | [4] Laxmi Shabadi, Snehal .T, Sanjana .H, Kalavati .G, Anita .K, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data using timer in Wireless Sensor Networks", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 3, June 2014. | [5] Xinyu Yang, Jie Lin, Paul Moulema,Wei Yu, Xinwen Fu and Wei Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems", 2012 32nd IEEE International Conference on Distributed Computing Systems | [6] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen, Fellow, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected | False Data in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 1, JANUARY 2012 | [7] K.Ren, W.Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (Mobi Hoc'05), pp 34-45,200515 | [8] Y.Zhang, W.Liu, W.Lou, and Y.Fang, "Location-Based Compromise-Toerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm. Vol.24,no.2,pp.247-260 Feb.2006. | [9] 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. | [10] S.He, J.Chen,Y.Sun, D.K.Y.Yau and N.K. Yip," On optimal information Capture by Energy-Constrained Mobile Sensors," IEEE Trans. Vehicular Technology, vol.59,no.5,pp.2472-2484,June 2010. |