ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

REPUTATION BASED ZONE TRUST DETECTION AND SWATT REVOCATION METHOD USING SPRT IN SENSOR NETWORKS

Rakshith Upparige K R [1], Sateesh Kumar H C [2]

PG Scholar, Department of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, Karnataka, India [1]

Associate Professor, Department of Telecommunication Engineering, Dayananda Sagar College Of Engineering, Bangalore, Karnataka, India [2]

Abstract: Wireless sensor networks can be used in several real world applications, including various critical applications such as military surveillance, infrastructure security monitoring and fault detection. Typically sensors are deployed in large number in environments that may not be safe or easily accessible to humans. An adversary or attacker can modify the sensor nodes that operate in the harsh environment and thus can insert faulty data to mislead the whole network. Hence in order to reduce the damage occurred to the compromised sensor nodes, it is extremely important to detect and revoke them as early as possible. The main idea is to propose zone based node compromise detection and revocation scheme for sensor networks. This is achieved using reputation based trust management scheme and software based attestation technique. Software attestation technique has been proposed to verify the integrity of the code without physical access. Whereas Reputation-based Framework for Sensor Networks maintain reputation for other nodes. This reputation is used to evaluate the trustworthiness of other nodes, which in turn establishes a web of trust in the network, which is then used as an inherent aspect in predicting the future behaviour of nodes in the network. Thus the proposed scheme provides effective and robust compromised sensor node detection and revocation capability with little overhead.

Keywords: Node compromise detection, sequential analysis.

I. INTRODUCTION

When sensors are deployed for critical applications, securing these sensors is important. If a sensor is compromised, an attacker can reprogram the sensor to act on his/her behalf. For example, the attacker can cause the sensor to send incorrect information to hide some military activity or send false information about the location of certain troops. Therefore, it is important to verify that the static memory contents of the sensors have not been modified, that is, to attest the static memory contents (which includes programs, keys, and system configuration information) of the sensors.Sensor networks can be deployed in hostile environments where adversaries may be present. Since wireless sensor networks usually need to be controlled remotely by the network operator, they are often deployed in an unattended manner. The unattended nature of wireless sensor networks can be exploited by attackers. Specifically, an attacker can capture and compromise sensor nodes and launch a variety of attacks by leveraging compromised nodes. To minimize the damage incurred, the system should detect and revoke them as soon as possible. The various node compromise detection schemes are: Reputation-based trust management schemes in which it identify malicious nodes but do not revoke them. Software-attestation schemes in which it require each sensor node to be attested periodically, which would incur substantial overhead. To mitigate the limitations of previous schemes, a zone-based compromise detection scheme in sensor network is framed. The main idea of the proposed scheme is to use sequential hypothesis testing to detect suspect regions in which compromised nodes are likely placed. In these suspect regions, nodes perform software attestation, leading to the detection and revocation of the compromised nodes. In software attestation based scheme it has been proposed to attest flash image codes and detect subverted image codes of compromised sensor nodes. They require each sensor node to be periodically

attested, as it cannot be predicted when the attacker will compromise sensors. But this periodic attestation will incur substantial overhead in terms of computation and communication.

II. RELATED WORK

S. Ganeriwal et al., [1] proposed Reputation-based Framework for Sensor Networks (RFSN) where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness, for which they employ a Bayesian formulation, specifically a beta reputation scheme, for reputation representation, updates and integration. F. Li et al., [2] presents Evaluating and quantifying stimulates collaboration in mobile ad hoc networks (MANETs). Existing reputation system sharply divides the trust value into right or wrong, thus ignoring another core dimension of trust: uncertainty. It deeply impacts a node's anticipation of others behaviour and decisions during interaction. T. Park et al., [3] discussed a Program- Integrity Verification (PIV) protocol that verifies the integrity of the program residing in each sensor device whenever the device joins the network or has experienced a long service blockage. The heart of PIV is the novel randomized hash function. A. Seshadri et al., [4] addresses SoftWare-based ATTestation for Embedded Devices (SWATT) is a technique for externally verifying the code, static data and configuration settings of an embedded device. M. Shaneck et al., [5] explained Remote Software-based Attestation for wireless Sensors over the network without requiring physical contact with the sensor. This scheme which achieves this goal by sending a check summing routine to the sensor from the base station. This code is protected by the techniques of encryption, obfuscation and self-modifying code, so that an attacker is unable to return a valid response from a compromised sensor within the allowed time. Y. Sun et al., [6] described a framework to quantitatively measure trust, model trust propagation, and defend trust evaluation system against malicious attacks. This system is employed in ad hoc networks for securing ad hoc routing and assisting malicious node detection. Y. Yang et al., [7] present a distributed software-based attestation for node compromise detection in sensor networks. This scheme is based on a pseudorandom noise generation mechanism and a lightweight block-based pseudorandom memory traversal algorithm. J. Jung et al., [8] explained Fast Port scan Detection Using Sequential Hypothesis Testing. Attackers routinely perform random "port scans" of IP addresses to find vulnerable servers to compromise. Network Intrusion Detection Systems (NIDS) attempt to detect such behaviour and flag these port scanners as malicious. In this paper they use traces from two sites to develop and assess their detection algorithm. H. Chan et al., [9] proposed random key predistribution schemes for sensor networks. Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystem are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. F. Delgosha et al., [10] described a novel multivariate key pre-distribution scheme (MKPS) that simultaneously provides many nice features of previous schemes without any disadvantages such as additional memory. These features include node-to-node authentication, network scalability, key compositeness, perfect secrecy up to the capture of a fraction of nodes, and network connectivity. In this scheme they assign n tuples of positive integer to the sensor nodes as their IDs. These IDs are used to distribute the shares of multivariate polynomials to the nodes prior to the network deployment. After the deployment, some nodes are able to directly establish n-1 common keys using the shares of polynomials stored in their memories. The secret key between these nodes is a combination of all these n-1 keys. Hence, the proposed scheme is, in a sense, an (n-1)-composite method. This feature considerably improves the security in the MKPS

III. PROBLEM DESCRIPTION

In this paper, attacker can simply monitor a significant fraction of the network traffic that would pass through these compromised nodes. Alternatively, he could inject falsified data to corrupt monitoring operation of the sensors. A more aggressive attacker could undermine common sensor network protocols, including cluster formation, routing, and data aggregation, thereby causing continual disruption to the network operations. Therefore, an adversary with compromised nodes can paralyse the deployed mission of sensor networks. In this sense, it is very important to detect and revoke compromised nodes as soon as possible in the network.

IV. EXISTING SYSTEM

Reputation-based trust management schemes have been proposed to manage an individual node's trust in accordance with its activities. In Reputation-based trust management schemes, malicious nodes can be identified, but they are not easily revoked due to the risk of false positives. Software-attestation based schemes achieve high node compromise detection capability, they require each sensor node to be periodically attested,

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

and as it cannot be predicted when the attacker will compromise sensors. This periodic attestation will incur substantial overhead in terms of computation and communication.

V. PROPOSED SYSTEM

Proposed a reputation-based trust management scheme that is designed to facilitate fast detection and revocation of compromised nodes. The key idea of our scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised. Specifically, we first divide the network into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Sequential Probability Ratio Test (SPRT). The SPRT decides a zone to be untrustworthy if the zone's trust is continuously maintained at low level or is quite often changed from high level to low level. Once a zone is determined to be untrustworthy, the base station or the network operator performs software attestation against all nodes in the untrustworthy zone, detects compromised nodes with subverted software modules, and physically revokes them.

A. PROPOSED SYSTEM ARCHITECTURE

Fig. 1 represents the overall flow of the project. First the network is divided into set of zones and a trust level is established with each zone to detect untrustworthy zones using sequential probability ratio test (SPRT). Once the zone is determined to be untrustworthy, the base station or network operator performs software attestation against all nodes in the untrustworthy zone and detects compromised nodes present in that zone and physically revokes them.

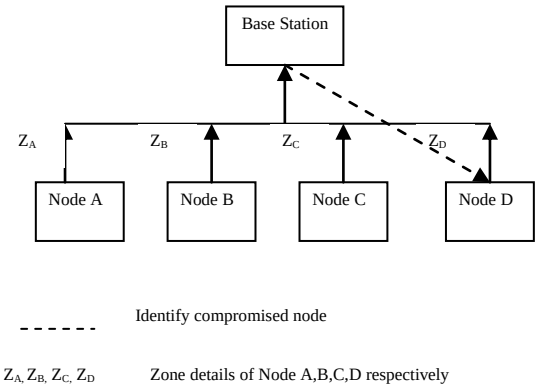


Fig 1: General system architecture

B. NORMAL NODE

Normal node in wireless sensor network is constructed in such a way that, it has its own id and key. The sensor node forwards the data to base station. Every mobile sensor node's movement is physically limited by the system configured maximum speed.

C. *ATTACKER NODE*

Attacker node is the compromised node, which is created by adversary. A mobile replica node u|, which has the same ID and secret key of normal mobile node u. An adversary creates compromise node by first compromising node u and extracts all secret keys from it. Then prepares a new node, sets the same ID as normal node and loads normal node's secret key. Under attacker models, we have three key design goals for compromised node detection. First, compromised nodes should be detected with minimal communication, computational, and storage overheads. Second, the detection schemes should be robust and highly resilient against the attacker's attempt to break the scheme. Finally, compromised node detection should be performed at the cost of minimal false positives and negatives.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

D. ZONE DISCOVERY AND TRUST AGGREGATOR SELECTION

After deployment, every sensor node u finds out its location and determines the zone to which it belongs. We call this zone the home zone. From u's point of view, we call other zones the foreign zones. Node u discovers every other node residing in the same zone. After the zone discovery process, the Trust Aggregator (TA) is selected in a round robin manner. Each and every mobile sensor node u generates zone discovery process $\{u||Z||T||MAC_{ku}\}$ and sends it to a neighbouring node v, where u, is the node identity, Z is the zone, T is the Time and MAC_{ku} is the key generated for node u. Each time a mobile sensor node u moves to a new location, it first discovers its distance.

E. TRUST FORMATION AND FORWARDING

For each time slot Ti, each node u in zone Z computes neighbourhood trust that is defined in accordance with the difference between the probability distributions of the information generated by u and the information sent to u by u's neighbouring nodes in zone Z. Base station receive zone discovery and TA value from the mobile sensor nodes. Upon receiving the details, the base station verifies the authenticity of the received details with the public key of node u and discards the claim if it is not authentic.

F. DETECTION AND REVOCATION

Upon receiving a zone-trust report from a TA in zone Z, the base station verifies the authenticity of TA's report with the secret shared key between TA and itself and discards the report if it is not authentic. A straightforward approach for untrustworthy zone detection is to decide a zone as untrustworthy by observing single evidence that its trust value is less than a predefined threshold. Base station receives zone discovery and trust aggregator from sensor nodes, then it verifies the authenticity of the received details with the key of node u and discards the details if it is not authentic.

VI. ASSUMPTION, THREAT MODEL AND REQUIREMENTS

A. ASSUMPTIONS

The base station is assumed to be secure and it will play the role of an attester in our discussion. In reality, any legitimate entity that shares a pair wise key with the sensor can be an attester. The communications between the base station and the sensors is secure using a pair wise key shared between them. The attester knows the hardware architecture and the original memory contents of the sensors. We assume that the sensors do not have virtual memory, as an attacker can modify the memory map, distinguish between data loads and instruction loads as pointed and evade our attestation. We argue that this assumption is reasonable, since state of the art micro-controllers do not have virtual memory support. The attester can communicate with all the sensors directly. We also assume that the attester can send a binary executable to the sensor and cause it to be executed.

B. THREAT MODEL

We assume that if the sensor is compromised, then the attacker has complete read-write access to the sensor's memory contents, including cryptographic keys, and is able to modify the memory contents at will. Thus, he can perform any type of software based attack on the attestation routine including static analysis (resulting in modification) of the routine, or software emulation of a sensor on a sensor. However, we assume that the attacker cannot tamper with the hardware of the sensor. Detection of attacks that involve external resources (such as the impersonation attack) requires hardware support and is considered to be out of scope. We assume that the attacker can perform a restricted form of collusion attack, which we call as the staging attack. We assume that the attacker can execute the attestation routine in stages. For example, a sensor with some modified portion of the memory can collude with the second sensor with a different modified portion of the memory. Each sensor runs the routine in such a way that it generates checksum on their respective un modified memory

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

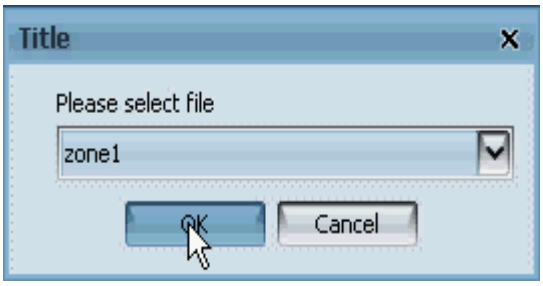
and then combines their checksums in the end to generate a valid checksum. Finally, the attacker can perform passive attacks such as eavesdropping, and active attacks such as replaying packets.

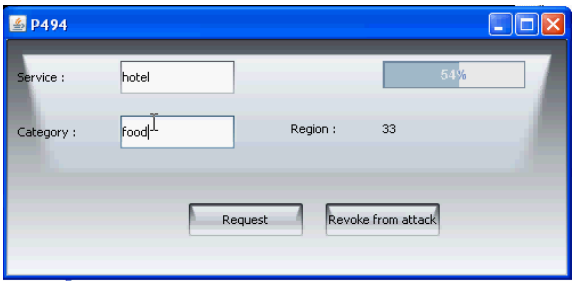
C. REQUIREMENTS

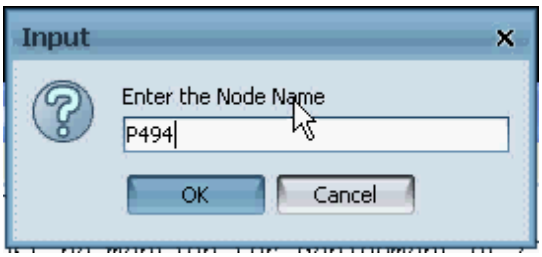
The attestation procedure should satisfy the following requirements.
Resistance to Replay: The attacker should not able to send a valid checksum to the verifier by simply reply--ing previous valid results.
Resistance to Prediction: The attacker should not be able to predict the next attestation routine. If the attacker can successfully predict the next attestation routine, then he can pre-compute the checksum.
Resistance to static analysis: The attacker should not be able to successfully analyze the code by using static analysis techniques within the time period the attester waits for a response from the sensor. This requirement will prevent the attacker from predicting the sequence of memory reads as well as predicting the location of read instructions in the attestation routine.
Very loose dependence on execution time: Since the attestation routine is sent over the network, it will be impossible for the attester to measure the actual execution time of the attestation routine. Therefore, the detection mechanism should not be dependent on the precise measurement running time of the attestation routine.
Complete memory coverage: To detect even small memory changes, the attestation routine should read every memory location.
Efficient construction: The attestation routine should be as small as possible to reduce bandwidth consumption and should be as efficient as possible to consume less battery power.

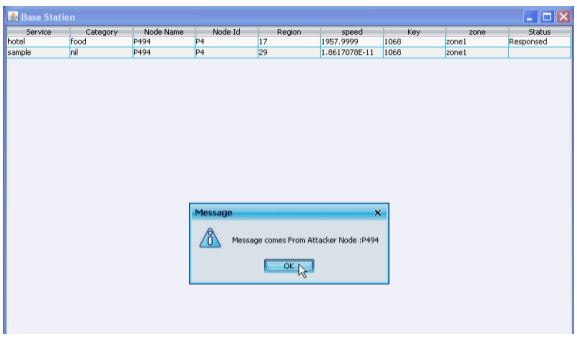
Further, the attestation routine should not introduce any new vulnerability in the system.

VII. RESULTS



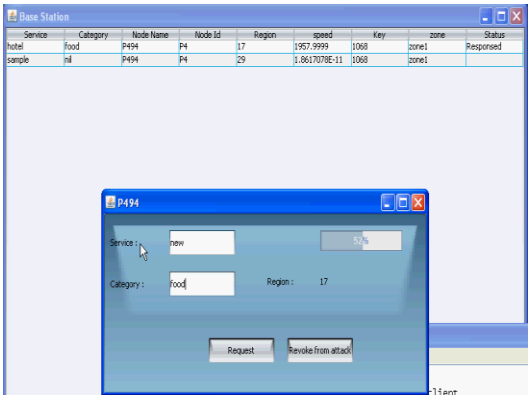


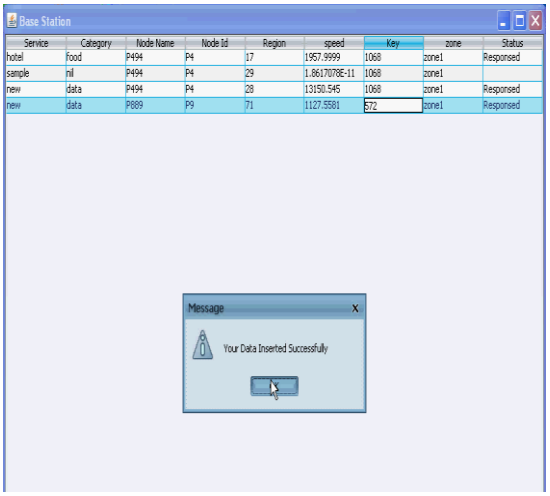




ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013





VIII. CONCLUSION

In this paper, we have proposed a zone-based node compromise detection and revocation scheme for sensor networks using the SPRT. We also enhanced the robustness of the SPRT with biased sampling. We have shown that our scheme achieves robust untrustworthy zone detection capability even if a majority of nodes in each zone are compromised. Furthermore, we have proposed countermeasures against the attacks that might be launched to disrupt the proposed scheme. We also modelled the interaction between the defender and the adversary as a repeated game with complete information and found a Nash Equilibrium. We show that the defender greatly limits the gains of the adversary under the Nash Equilibrium. We evaluated the proposed scheme through simulation experiments under various scenarios. Our experimental results show that our scheme quickly detects untrustworthy zones with a small number of zone-trust reports.

REFERENCES

[1] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", *ACM SASN*, October 2004.

[2] F. Li and J. Wu,"Mobility reduces uncertainty in {MANETS}", *Proc. IEEE 26th Int'l Computer communications Conf,* pp. 1946-1954, May 2007.

[3] T. Park and K. G. Shin. "Soft tamper-proofing via program integrity verification in wireless sensor networks", *IEEE Trans. Mobile Computi*ng, Vol 4, Issue 3, pp. 297-309, 2005.

[4] A. Seshadri, A. perrig, L. Van Doorn, and P. Khosla "{SWATT}: SoftWare-based ATTestation for Embedded Devices", *Proc. IEEE Symp*. pp. 272-282, May 2004.

[5] M. Shaneck, K. Mahadevan, V. Kher, and Y. Kim "Remote Software-based Attestation for wireless Sensors", In *ESAS*, pp. 27-41, July 2005.

[6] Y. Sun, Z. Han, W. Yu, and K. Liu "A trust evaluation framework in distributed networks: vulnerability analysis and defence against attacks", *Proc. IEEE 25th Int'l Computer communications Conf,* pp. 1-13, April 2006.

[7] Y. Yang, X. Wang, S. Zhu, and G. Cao "Distributed software-based attestation for node compromise detection in sensor networks", *Proc. IEEE Symp. Reliable Distributed Systems*, pp. 219-230, October 2007.

[8] J. Jung, V. Paxson, A.W. Berger, and H. Balakrishnan "Fast port scan detection using sequential hypothesis testing", *Proc. IEEE Symp. Security and Privacy*, pp. 9-12, May 2004.

[9] H. Chan, A. Perrig, and D. Song "Random key predistribution schemes for sensor networks", *Proc. IEEE Symp. Security and Privacy*, pp. 197-213, May 2003.

[10] F. Delgosha and F. Fekri "Threshold key-establishment in distributed sensor networks using a multivariate scheme", *Proc. IEEE 25th Int'l Computer communications Conf,* pp. 1-12, April 2006.