

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 10-02-2010		2. REPORT TYPE Final Report		3. DATES COVERED (From - To) 27-Jun-2005 - 26-Jun-2009	
4. TITLE AND SUBTITLE Distributed Self-healing Mechanisms for Securing Sensor Networks			5a. CONTRACT NUMBER W911NF-05-1-0270		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 611102		
6. AUTHORS Sencun Zhu, Guohong Cao, Peng Liu			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Pennsylvania State University Office of Sponsored Programs The Pennsylvania State University University Park, PA 16802 -			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 48423-CS.1		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT The specific goal of this proposal is to design and implement efficient self-healing mechanisms that allow a sensor network to recover from node compromises by itself. To achieve this goal, this proposal describes a self-healing framework that consists of three sequential phases: node compromise detection, node revocation and network reconfiguration, and focuses on designing efficient schemes for each of these phases. It proposes to identify suspicious sensor nodes through time synchronization protocols and location changes of sensor nodes,					
15. SUBJECT TERMS Self-healing, Key management, Authentication, Software attestation, Compromise Detection					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Sencun Zhu
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 814-865-0995

Report Title

Distributed Self-healing Mechanisms for Securing Sensor Networks

ABSTRACT

The specific goal of this proposal is to design and implement efficient self-healing mechanisms that allow a sensor network to recover from node compromises by itself. To achieve this goal, this proposal describes a self-healing framework that consists of three sequential phases: node compromise detection, node revocation and network reconfiguration, and focuses on designing efficient schemes for each of these phases. It proposes to identify suspicious sensor nodes through time synchronization protocols and location changes of sensor nodes, respectively, in addition to other sources of discovering suspicious nodes. It then investigates techniques to attest the authenticity of the code running in the suspected nodes to check if the suspected nodes are really compromised. Two key updating schemes, one for group key updating and the other for pairwise key updating, are proposed to invalidate the security keys possessed by the nodes that have been identified as compromised.

List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

- (1) H. Song, S. Zhu, W. Zhang, and G. Cao. Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks. In ACM Transaction on Sensor Networks (TOSN), Vol.4-4, Nov. 2008.
- (2) W. Zhang, S. Zhu, and G. Cao. Predistribution and local collaboration-based group rekeying for wireless sensor networks Ad Hoc Networks, Volume 7, Issue 6, August 2009.
- (3) M. Shao, S. Zhu, W. Zhang, G. Cao, Y. Yang. pDCS: Security and Privacy Support for Data-Centric Sensor Networks. IEEE Transactions on Mobile Computing, Volume 8, Number 8, August 2009.

Number of Papers published in peer-reviewed journals: 3.00

(b) Papers published in non-peer-reviewed journals or in conference proceedings (N/A for none)

Number of Papers published in non peer-reviewed journals: 0.00

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts): 0

Peer-Reviewed Conference Proceeding publications (other than abstracts):

- (1) Y. Yang, S. Zhu, G. Cao, and T. LaPorta. An Active Global Attack Model for Sensor Source Location Privacy: Analysis and Countermeasures. Proceedings of International Conference on Security and Privacy in Communication Networks (Securecomm), 2009.
- (2) M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurthy, T. La Porta. Cross-layer Enhanced Source Location Privacy in Sensor Networks Proceedings of the 6th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2009).
- (3) G. Ruan, S. Jain, and S. Zhu. SensorEar: A Sensor Network Based Eavesdropping System. Workshop on Embedded Systems and Communications Security, in conjunction with SRDS 2009.
- (4) M. Shao, S. Zhu, G. Cao, T. La Porta and P. Mohapatra. A Cross-layer Dropping Attack in Video Streaming over Ad Hoc Networks. In Proc. of International Conference on Security and Privacy in Communication Networks (Securecomm), 2008.

(d) Manuscripts

Number of Manuscripts: 0.00

Number of Inventions:

Graduate Students

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
Yi Yang	1.00
FTE Equivalent:	1.00
Total Number:	1

Names of Post Doctorates

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>	National Academy Member
Sencun Zhu	0.08	No
FTE Equivalent:	0.08	
Total Number:	1	

Names of Under Graduate students supported

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

- The number of undergraduates funded by this agreement who graduated during this period: 0.00
- The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00
- The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00
- Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00
- Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00
- The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00
- The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

<u>NAME</u>
Total Number:

Names of personnel receiving PHDs

<u>NAME</u>
Liang Xie
Total Number: 1

Names of other research staff

<u>NAME</u>	<u>PERCENT SUPPORTED</u>
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Final Report

Award Number: W911NF-05-1-0270

1. Statement of Problem

When sensor networks are deployed in an unattended and hostile environment such as a battlefield, sensor nodes must be furnished with cryptographic mechanisms to protect the confidentiality and authenticity of sensor readings from being jeopardized by an adversary. Cryptography, however, can only provide the first layer of protection. The low cost of sensor nodes (e.g., less than \$1 as envisioned for smart dust) precludes the built-in tamper-resistance capability of sensor nodes. Actually, recent advances in physical attack show that even memory chips with built-in tamper-resistance are subject to various memory read-out attacks. Thus, the lack of tamper-resistance coupled with the unattended nature gives an adversary the opportunity to break into the captured sensor nodes to obtain the code and the sensitive information such as encryption or authentication keys loaded in these sensor nodes. An adversary may change the original code to malicious code, and it may deploy many cloned malicious nodes with the obtained keys. The cloned nodes can participate in the network to launch various kinds of passive and active security attacks.

Recently several preventative security mechanisms have been proposed to restrict the security impact of node compromises to one-hop range of the compromised nodes and filter out false sensor readings injected into the network by a certain number of compromised colluding nodes. Despite the increased complexity and performance overhead, these schemes do not solve the node compromise problem completely. When the number of compromised nodes exceeds the security threshold in these schemes, an adversary can break the system and easily launch security attacks. To fully address the node compromise problem, we believe that it is essential to detect the compromised nodes in a timely fashion and isolate them from the rest of the network. It is desired that a sensor network have the self-healing capability so that the security of the system will not be broken even after a relatively high number of sensor nodes have been compromised. With the self-healing capability, a sensor network can employ lightweight prevention techniques to reduce the normal operational overhead.

2. Summary of The Most Important Results

To achieve the design goals, we have developed through this project a suite of security mechanisms spanning node compromise detection, verification, and revocation.

2.1: Direct Results from this project

- based on verifying the genuineness of the running program, we propose two distributed software-based attestation schemes that are well tailored for sensor networks. These schemes are based on a pseudorandom noise generation mechanism and a lightweight block-based pseudorandom memory traversal algorithm. Each node is loaded with pseudorandom noise in its empty program memory before deployment, and later on multiple neighbors of a suspicious node collaborate to verify the integrity of the code

containing sensor worms. Our work is the first one proposing countermeasures towards sensor worms. [Yi et al., Mobihoc 2008]

- we studied the problem of node cloning attacks in sensor networks. The defenses against clone attacks are not only very few, but also suffer from selective interruption of detection and high overhead (computation and memory). We propose a new effective and efficient scheme, called SET, to detect such clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbors in the network in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. SET then employs a tree structure to compute non-overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. Randomization is used to further make the exclusive subset and tree formation unpredictable to an adversary. Performance analysis and simulations also demonstrate that the proposed scheme is more efficient than existing schemes from both communication and memory cost standpoints. [Choi et al., Securecomm 2007]
- We also studied secure sensor data aggregation. Hop-by-hop data aggregation is a very important technique for reducing the communication overhead and energy expenditure of sensor nodes during the process of data collection in a sensor network. However, because individual sensor readings are lost in the per-hop aggregation process, compromised nodes in the network may forge false values as the aggregation results of other nodes, tricking the base station into accepting spurious aggregation results. Here a fundamental challenge is: how can the base station obtain a good approximation of the fusion result when a fraction of sensor nodes are compromised? To answer this challenge, we proposed SDAP [Yi et al., Mobihoc'06, TISSEC'08], a Secure Hop-by-hop Data Aggregation Protocol for sensor networks, based on the principles of divide-and-conquer and commit-and-attest. SDAP can achieve the level of efficiency close to an ordinary hop-by-hop aggregation protocol while providing certain assurance on the trustworthiness of the aggregation result.
- Another important issue we studied is tolerating mobile sink compromises [Song et al., Mobihoc'05, TOSN'08]. Mobile sinks are dispatched to perform critical actions (e.g., collecting data, node revocation) in a sensor network, so their compromises will have catastrophic impacts on sensor applications. We were the first one studying this problem and came up with effective solutions based on the principles of least privilege to minimize the impact of mobile sink compromises.

2.2: Additional Results with partial support from this grant

- For sensor networks deployed to monitor and report real events, event source location privacy is an attractive and critical security property, which unfortunately is also very difficult and expensive to achieve. This is not only because adversaries may attack against sensor source privacy through traffic analysis, but also because sensor networks are very limited in resources. Partially supported by this project, we also developed several schemes for sensor source location privacy.

Specifically, we first studied source location privacy for sensor networks under a global observer who may monitor and analyze the traffic over the whole network. We employ

Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2009.

7. Y. Yang, S. Zhu, and G. Cao. "Improving Sensor Network Immunity under Worm Attacks: A Software Diversity Approach." In *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2008.
8. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. "Towards Event Source Unobservability with Minimum Network Traffic in Sensor Networks." In *The ACM Conference on Wireless Network Security (WiSec)*, 2008.
9. M. Shao, Y. Yang, S. Zhu, and G. Cao. Towards Statistically Strong Source Anonymity for Sensor Networks. in *IEEE International Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, 2008.
10. Y. Yang, X. Wang, S. Zhu, and G. Cao. "Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks." *Proceedings of 26th IEEE International Symposium on Reliable Distributed Systems (SRDS)*, Oct. 2007.
11. H. Song, L. Xie, S. Zhu, and G. Cao. "Sensor Node Compromise Detection: The Location Perspective." In *Proc. of International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2007.
12. H. Choi, S. Zhu, and T. Laporta. "SET: Detecting node clones in Sensor Networks." *Proceedings of International Conference on Security and Privacy in Communication Networks (SecureComm)*, Sept. 2007.
13. M. Shao, S. Zhu, W. Zhang, and G. Cao. "pDCS: Security and Privacy Support for Data-Centric Sensor Networks." in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, May 2007.
14. Y. Yang, X. Wang, S. Zhu, and G. Cao. "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks." In *Proc. of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, May 2006.
15. Hui Song, Sencun Zhu, and Guohong Cao. "Attack-Resilient Time Synchronization for Wireless Sensor Networks." In *Proc. of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'05)*, 2005.
16. Wensheng Zhang, Hui Song, Sencun Zhu, and Guohong Cao. "Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks." In *Proc. of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05)*, May 2005.