Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.222 – 227

CLUSTER BASED DYNAMIC KEYING TECHNIQUE FOR WIRELESS SENSOR NETWORK

[1]P.B.Arun Prasad, M.E.(CSE).**, [2]R.Ramanikumari, [3]K.Raveena, [4]K.Selva Bharathi, [5]P.Siva Bharathi**

ABSTRACT: In heterogeneous wireless sensor networks the mobility of sensor node become essential for various applications. There is a possibility for the malicious node to occur. This causes the cluster or the whole network to be controlled by the malicious node .The mobile sensor nodes need to be authenticated; further clustering of nodes improves scalability, energy efficient routing and data delivery. The nodes with high configuration are chosen as cluster head based on weight values which is estimated using parameters such as node degree, average distance, average speed and virtual battery power. The keys are generated using dynamic clustering efficiency algorithm. Hierarchical trust management protocol is used for finding the malicious node among the group of sensor nodes.

Keywords: Wireless Sensor, malicious node, Hierarchical trust, cluster and battery.

A. INTRODUCTION

Wireless sensor networks hold great promise as an enabling technology for a variety of applications. Data collection and event detection are two such classes of applications that are broadly representative and which have received considerable attention in the literature. While wireless multi-hop data collection has achieved operational lifetimes on the order of a year, we are unaware of lifetimes exceeding a few days or weeks for wireless multi-hop event detection sensor networks. This project is that sensor networks for event detection are constrained by two factors which do not similarly affect data collection sensor networks. The first factor is that no appropriate sensing, signal conditioning, and signal processing

architecture has been broadly implemented to support event detection in distributed systems that are simultaneously energy, space, time, and message complexity-constrained. The second factor is that middleware for services such as time synchronization, localization, and routing are predominantly and unnecessarily proactive.

A comparison of data collection and event detection will serve to illustrate the subtle but important differences between these applications. Fundamentally, data collection is a signal reconstruction problem in which the objective is to centrally reconstruct observations of distributed phenomena with high spatial and temporal fidelity. Performance metrics for such applications include the accuracy and precision of the signal reconstruction, the correlation between the observed signal and the underlying physical phenomena, and the lifetime of the sensor network.

Physical phenomena such as light, temperature, humidity, and barometric pressure change at very low frequencies and can be sampled faithfully at periods of a minute or more. System performance can be adjusted by introducing compression and aggregation, or by varying the duty-cycle, sampling and communication rates, allowing sensor lifetimes to approach a year or more. In contrast with data collection, sensor network applications for event detection must continuously observe noise for the rare presence of a burst of high-frequency signal.

B. EXISTING SYSTEM

All existing approaches in this category detect replicas based on finding conflicting location claims. The first one is Node-To-Network Broadcasting. When executing the protocol, each node broadcasts its location claim to the whole network, and all nodes store the location claims of their neighbours only. Then if a node receives two conflicting claims of some node ID, it can revoke that node by flooding the network with the two claims.

The second approach is Deterministic Multicast. A fixed mapping function is used to map each node ID to g nodes (witness nodes), and then each node's neighbours will forward the node's location claim to these *g* nodes.

In Randomized Multicast the neighbours of each node randomly select *n* nodes as that node's witnesses. Then if a node is replicated, according to the birthday paradox problem, at least one witness will receive two conflicting location claims with high probability. LSM improved on Randomized Multicast.

In LSM the nodes in the paths from a node's neighbours to the randomly selected witnesses are used; these nodes become the node's witnesses too. Such change reduces the communication cost.IN SDC Each node ID is mapped to one cell, and the location claim of each node is forwarded to the mapped cell and broadcasted within the cell. Nodes in the cell store the claim and become that node's witnesses with some probability. However, the set of possible mapped cells is still deterministic. In cloning attacks, an adversary captures a sensor node, reprograms it, makes multiple copies, and inserts these copies, into the network. Cloned nodes subvert sensor network processing from within. In a companion paper we show how to detect and remove clones from sensor networks using random key predistribution security measures. Keysthat are present on the cloned nodes are detected by using authentication statistics based on key usage frequency. For consistency with existing random key predistribution literature, and ease of explanation, the network in that paper used an Erdos-Renyitopology.

In the Erdos-Renyi topology, the probability of connection between any two nodes in the network is uniform. Since the communications ranges of sensor nodes are limited, this topology is flawed. This article applies the clone detection approach from] to more realistic network topologies. Grid and ad hoc topologies reflect the node connectivity patterns of networks of nodes with range limits. We provide analytical methods for choosing detection thresholds that accurately detect clones. We use simulations to verify our method. In particular we find the limitations of this approach, such as the number of nodes that can be inserted without being detected.

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighbourhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties [10], i.e., properties that arise only through the collective action of multiple nodes. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware,

distributed node-replica detection, and Line-Selected Multicast displays particularly strong performance characteristics. We show that emergent algorithms represent a promising new approach to sensor network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

C. PROPOSED SYSTEM

The proposed system shows that in order to avoid the drawbacks of existing approaches, replica-detection protocols must be non deterministic and fulfill three security requirements on witness selection. To our knowledge, Randomized Multicast is the only existing protocol fulfilling the requirements, but it has very high communication overhead (i.e., O(n) per node). Secondly, based on random walk, we propose two new protocols fulfilling the requirements, while having only moderate communication and memory overheads. Our random walk strategy outperforms previous strategies because it naturally distributes the responsibility of witness node selection to every passed node of random walks, and then adversaries cannot easily find out the critical witness nodes.

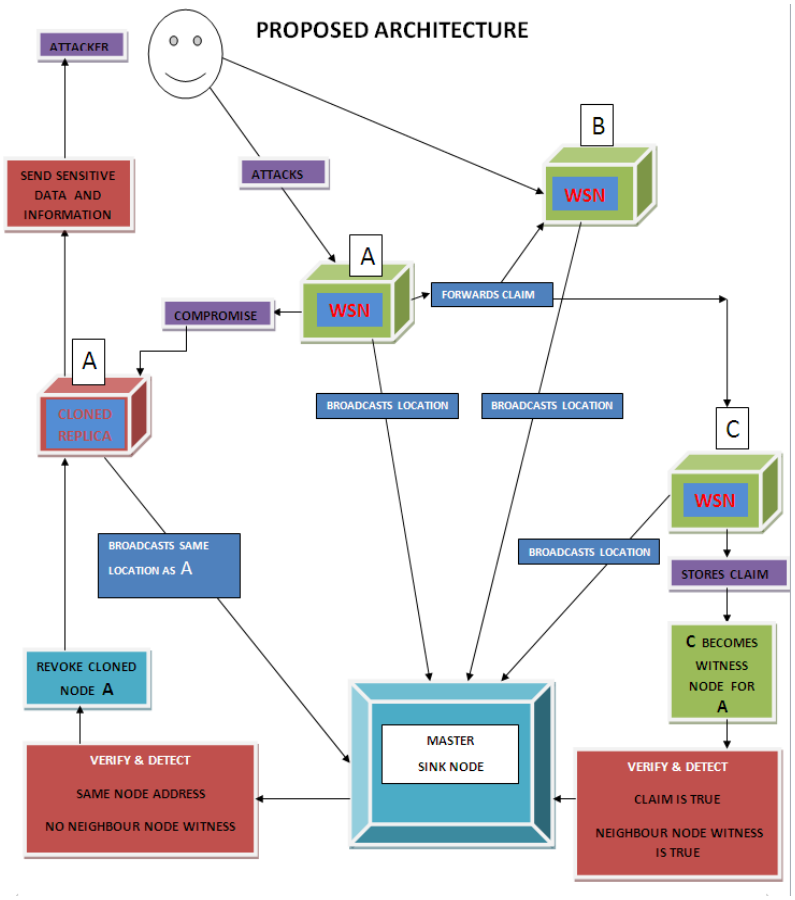

Fig 1.Proposed Architecture

The protocol, RAndom WaLk (RAWL), starts several random walks randomly in the network for each node a, and then selects the passed nodes as the witness nodes of node a. Our analysis shows that walk steps are sufficient to detect clone attacks with high probability. The second protocol, Table-assisted RAndom WaLk (TRAWL), is based on RAWL and adds a trace table at each node to reduce memory cost. Usually the memory cost is due to the storage of location claims; in TRAWL each node only stores O(1) location claims now (although the size of the trace table is still, the size of a table entry is much smaller than the size of a location claim).

D. WORKING PRINCIPLE

Wireless Sensor nodes are setup with information collection and dissemination to the sink or master node. The WSN are placed in a remote locations with a sink connected to the network. According to the number of cluster heads, the nodes are randomly placed in a network. As events occur randomly the WSNS transmit the data to the sink node or master node. AODV protocol is used for event transmission it forwards the event to the next hop based on the source and destination IP address. Each node is assumed to be calculating the energy independently. The data transmission takes places. Whenever the particular node is used for data transmission, an energy level should be reduced. The WSNs which act as relays also lose energy when relaying the datas of the WSN's. Thus each node is acting independently when event occurs and transmits energy according to differing energy levels. When the event is transmitted from one sensor node to another there is a possibility for the attacker to compromise that specific node and snoop the information. When the attack is initiated, the whole sensor nodes can be compromised and makes node to loss its energy and also loses its lifetime(nodes dead). The proposed system shows that in order to avoid the drawbacks of existing approaches, replica-detection protocols must be non deterministic and fulfill three security requirements on witness selection. For security purpose using virtual key and location coordinates protocols, this mechanism generates the dynamic key based on the node degree and coordinates. Another protocol used is hierarchical trust management to prevent the sensor nodes from the attacker. Trust-based IDS algorithm is based on selecting a system minimum trust threshold, *T th* below which a node is considered compromised and needs to be excluded from sensor reading and routing duties otherwise server will block the attacking entities.

CONCLUSION

Randomized Multicast, fulfills the requirements; however it has very high communication overhead which is only affordable in small networks than existing Another protocol LSM(line selected multicast) has the lowest communication and memory overheads, but it does not fulfill the security requirements. Our final protocols, RAWL(RAndom Walk) and TRAWL(Table-assisted RAndom WaLk), which are based on random walk, fulfill the requirements and have higher but comparable communication overhead than LSM. It provides a better trade-off between the communication overhead and security properties than previous protocols. We also gave theoretical analysis on the required number of random walk steps. Finally, the mechanism TRAWL also reduces the memory overhead.

REFERENCES

[1] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson. "Wireless Sensor Networks for Habitat Monitoring." ACM WSNA'02, 2002.
[2] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu. Energy-Efficient Surveillance System Using Wireless Sensor Networks. Mobisys, 2004.
[3] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton. "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care." Intl. Workshop on Wearable and
Implantable Body Sensor Networks, April 2004.
[4] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava. "Energy Aware Wireless Sensor Networks". IEEE Signal Processing 19, 2, 40--50.
[5] W. Yuan, S. V. Krishnamurthy, and S. K. Tripathi. "Improving the Reliability of Event Reports in Wireless Sensor Networks". ISCC, 2004.
[6] S. Madden, M. J. Franklin, and J. M. Hellerstein. TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Networks. OSDI, December 2002.
[7] D. Estrin, R. Govindan, J. S. Heidemann, S. Kumar. "Next Century Challenges: Scalable Coordination in Sensor Networks." MOBICOM 1999: 263-270
[8] TinyOS – http://www.TinyOS.net
[9] P. Levis, N. Lee, M. Welsh and D. Culler. TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications. ACM SenSys 2003.
[10] D. Gay, P. Levis and R.von Behren. "The nesC Language: A Holistic Approach to Networked Embedded Systems."
[11] The Network Simulator - ns-2 "http://www.isi.edu/nsnam/ns/".

