International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.4, pp.56-61, August (2018)
Research Paper
E-ISSN: 2320-7639

Detection of Node Capture Attack in Wireless Sensor Networks

K. Ravikumar[1], V. Manikandan[2*]

[1]Department of Computer Science, Tamil University, Tanjavurr, India
[2]Department of Computer Science, Tamil University, Tanjavurr, India

**Corresponding Authormanikandanskt1994@gmail.com*

Available online at: www.isroset.org

Accepted: 22/Aug/2018, Online: 31/Aug/ 2018

Abstract- A comprehensive analysis on connectivity and resilience of secure sensor networks under the widely studied q-composite key pre-distribution scheme. For network connectivity, which ensures that any two sensors can find a path in between for secure communication, we derive the conditions to guarantee connectivity in consideration of: 1) node-capture attacks, where the adversary may capture a set of sensors and compromise keys in their memory; 2) sensor mobility, meaning that sensors can move around so that the network topology may change over time; 3) physical transmission constraints, under which two sensors have to be within each other's transmission range for communication; 4) the boundary effect of network fields; and 5) link unreliability, meaning that links are allowed to be unreliable. In contrast, many prior connectivity analyses of secure sensor networks often ignore the above issues. For resilience, although limited studies have presented formal analysis, it is often assumed that the adversary captures a random set of sensors, whereas their paper allows the adversary to capture an arbitrary set of sensors. A present conditions to ensure unassailability and unsplittability in secure sensor networks under the q-composite scheme. Unassailability ensures that an adversary capturing any set consisting of a negligible fraction of sensors can compromise only a negligible fraction of communication links although the adversary may compromise communications between non-captured nodes, which happen to use keys that are shared by captured nodes. Unsplittability means that when a negligible fraction of sensors are captured, almost all of the remaining nodes are still securely connected. Based on the results of connectivity, unassailability, and unsplittability , to provide useful guidelines for the design of secure sensor networks.

Keywords- Sequential Analysis, Replica Detection, Wireless Sensor Network, Node capture attack, Event-Based Attack Decomposition

I. INTRODUCTION

1.1 Introduction to Wireless Sensor Network

Wireless sensor networks (WSN), from time to time describe wireless sensor and actuator set of connections, are spatially disseminated independent sensors to keep an eye on physical or ecological circumstances, such as hotness, sound, pressure, etc. and to cooperatively pass their data through the network to other locations. The additional modern set of connections are bi-directional, also facilitate control of sensor movement. The development of wireless feeler set of connections was maddened by military applications such as battle ground observation; today such networks are used in many developed and customer application, such as manufacturing process scrutinize and be in authority of, machine corporal condition monitor, and so on.

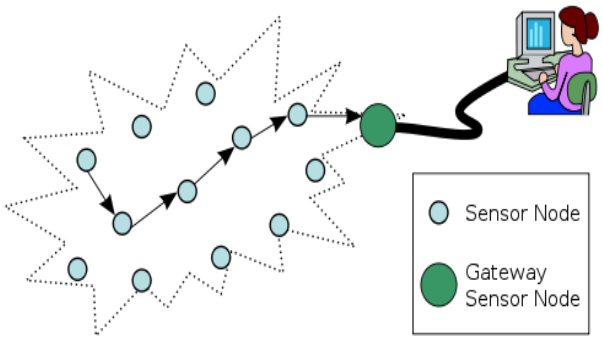

Figure 1.1 Wireless Sensor Network

Such a set of sensor node connections has typically quite a lot of parts:

A microcontroller, association to an external antenna, a radio transceiver with an internal transmitter or an electronic circuit for interfacing with the sensors and an get-up-and-go source, usually a battery or an entrenched form of energy

produce. This sensor nodes may vary of the size of a shoebox down to the size of a grain of dusts, even though functioning "motes" of beyond doubt microscopic magnitude have yet to be created. The asking price of sensor nodes in the similar way to changeable, range from a few to hundreds of dollars, depending on the complexity of individualing sensor nodes. Measurements and cost restraint on their sensor nodes may result in correspond able constraint on their possessions such as memory, power, computational speeds and infrastructures bandwidth. The topology of the WSNs can vary from an undemanding star network to an advanced multi-hop wireless mesh multifaceted. The proliferation technique between the hops of the set of family members can be direction-finding or deluge.

1.2Problem statement

In random key pre-distribution (RKP) scheme, a large pool of accidental symmetric keys and their ids is produce, and then every node is assign with a number of keys arbitrarily selected from a pool. After deployment, nodes transmit ids of keys along with their node id to neighbors to conclude their shared pair wise keys. If the set of connections density, the size of the key pool, and the number of keys assign to each sensor node are carefully chosen, then it can be ensured with high probability that all the bordering nodes in the network will share at least one key with each other. While pre-distributing pair wise keys does protect discretion, it still loads nodes with a large quantity of globally-applicable secrets. By do away with the eavesdropping attack, the pair wise scheme makes another type of malevolent behavior more attractive. As several nodes possess the same keys; any node can make use of them. Basically come jointly the keys obtained from a momentous number of collaboration nodes greatly increase the attacker's probability of sharing keys with other nodes. A secret attacker could share its pair wise keys between compromised nodes, easy approach each to present multiple 'authenticated' characteristics to other nodes while avoiding for detection. In order to counter the collusion attack, nodes should destroy unused keys from the node memory after an initialization phase, but this means new nodes can no longer join the system once initialization is complete.

II. REVIEW OF LITERATURE

A Randomized, Efficient, and Distributed (RED) protocol was future to enhance the line selected multicast scheme of in terms of copy detection probability, storage and calculation overheads (J. Ho, D. Liu[7]).

However, RED still has the same communication overhead as the line-selected multicast scheme. More significantly, their protocol requires repeated position claims over time, meaning that the cost of the scheme needs to be multiplied by the number of runs during the total deployment time. Contained multicast schemes based on the grid cell topology detect replicas by letting location claim be multicast to a single cell or manifold cells. The main strength of is that it achieves advanced detection rates than the best arrangement. However, has similar communication overheads as.

A clone discovery scheme was proposed in sensor systems (L. Hu and D. Evans [8]). In this scheme, the network is considered to be a set of non-overlapping sub counties. An exclusive subset is formed in each sub region. If the connection of subsets is not empty, it implies that replicas are included in those subsets. Fingerprint-based replica node discovery scheme was proposed in sensor networks(J.Jung,V. Paxon [9]). In this scheme, nodes report fingerprints, which classify a set of their neighbors, to the base station. The base station achieves replica detection by using the property that impressions of replicas battle each other (K. Xing [10]).

III. PROBLEM DEFINITION

3.1.Network Models

Sensor systems are often deployed in an unattended manner, most of these protocols are exposed to a variety of attacks such as denial of facility attacks, routing disturbance and false data injection attacks, network service disturbance attacks. To defend the wireless sensor networks against these numerous attacks, many arrangements have been industrialized in the works. For instance, secure routing schemes have been proposed to alleviate routing disruption attacks. False data injection attacks can be alleviated by using the authentication schemes. Secure data combination protocols are used to stop attacker from disrupting combination. Many schemes have also been proposed to protect localization and time synchronization protocols from the threat.

It first assumes a static instrument network in which the positions of sensor nodes do not change after deployment. It also assumes that every instrument node works in promiscuous mode and is able to identify the sources of all messages originating from its neighbors. We believe that this assumption does not incur considerable overhead because each node inspects only the source IDs of the communications from its neighbors rather than the entire fillings of the messages.

3.2. Attacker Models

By assume that an attacker can physically capture sensor nodes to cooperation them. However, it places restrictions on the number of sensor nodes that he can physically capture in each target region. This is reasonable from the viewpoint that an increase in the number of the captured sensor nodes will lead to a rise in the probability that attacker is detected by intruder detection mechanisms. Therefore, a substance attacker will want to considerably

capture the limited number of instrument nodes in each target region while not being detected by intruder detection mechanisms. Moreover, assume that it takes a certain quantity of time from taking nodes o redeploying them in the network. This is reasonable in the sense that an attacker needs some time to cooperation captured instrument nodes.

The random key predistribution schemes is performed an evaluated with respect to the node capture resilience. It can be defined as the probability that a given secured link between two uncaptured nodes can be compromised by an attacker using keys extracted from already captured nodes. the node capture resilience is a fraction of secured links between uncaptured nodes that can be compromised by an attacker. The node capture resilience is mostly influenced by the following three factors – the ring size m, the key pool size |S| and the probability that any two nodes in the network can establish a link key. These values are to some extent determined by properties of the network concerned. The ring size m is limited by a storage capacity of the network sensor nodes. If we want the network to be connected by secure links, the minimum required probability of a link key establishment is given by the size of the network and by the average number of neighboring nodes. Given the m and the minimum required probability, the |S| is uniquely determined. Note that in the q-composite scheme also the q influences the node capture resilience and the key pool size |S|.

IV. PROPOSED SYSTEM

4.1 Node Capture Attack

In static sensor systems, a sensor node can be considered to be simulated if it is placed at more than one location. However, if nodes are allowed to freely roam through the network, the above method does not work because the mobile nodes location will unceasingly change as it moves. Hence, it is authoritative to use some other technique to detect imitation nodes in mobile sensor networks. Fortunately, movement provides us with a clue that can help resolution the mobile replica discovery problem. Specifically, a mobile sensor node should never move faster than the system-configured maximum speed. Consequently, if it notices that the mobile node "s speed is over the wide-ranging speed, it is then highly likely that at least two nodes with the same identity are present in the network.

Each period a moveable sensor node moves to a new position, each of its residents asks for a employed claim containing its location and time material and decides probabilistically whether to onward the conventional entitlement to the base station. The base position computes the speediness from every two uninterrupted claims of a mobile node and achieves the by taking speed as an experiential sample.

Each time highest speed is exceeded by the mobile node; it will accelerate the random walk to hit or cross the higher limit and thus lead to the base position accepting the alternative hypothesis that the moveable node has been simulated. On the other hand, each time the thoroughgoing speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus principal to the base station tolerant the null hypothesis that mobile node has not been replicated. Once the base position decides that a mobile node has been replicated, it initiates cancelation on the replica nodes.

It also assumes that every moveable sensor node is able to obtain its location information and verify the locations of its neighboring nodes. This can be applied by employing GPS. This assumption may not lead to additional costs if the location material is used for other purposes. Finally, undertake that the clocks of all nodes are loosely coordinated with a thoroughgoing error of. This can be accomplished by the use of secure time.

4.2 Event-Based Attack Decomposition

It proposes a method for the expansion of suitable performance metrics for node capture attacks by decomposing the attack goal into a collection of events. By spacing the attack tasks into a graphical structure, the value of certain events can be computed via graph composition as a function of the corresponding sub-event values. This goal is most likely to cause some sort of noticeable effect on the network and it is likely to be an arrangement of a number of attack events. By disintegrating the goal into these separate events, the adversary is better able to gauge the progress of the attack toward the desired goal. To further simplify the attack evaluation, suggest a further rottenness of attack events into simpler sub events, until a collection of easily described primitive attack events is obtained, noting that such decomposition need not be unique. The rottenness of the attack into these primitive events similarly allows for decomposition of the attack assessment metric into quantities that measure the value of achieving individual events. Once a set of nodes C has been captured, the attack presentation metric can be evaluated by recombining the values of the achieved primitive events by reversing the original putrefaction.

It consists of three phases:

(i) Key pre-distribution phase
(ii) Shared-key discovery phase
(iii) Path-key establishment phase

The first and third phase is exact similar to the Du-Deng-Han-Varshney-Distribution (DDHV-D) scheme.

The second phase differ at since the Modified Bloom's Scheme is used for the key generation.

Phase 1: Key Pre-distribution Key pre-distribution phase

This can be performed before the sensors are deployed in the area under surveillance. As in DDHV-D scheme, the key-space pool S is divided into t x n key-space pools Si,j (for i=1, . . . , t and j=1, . . . , n), with Si,j corresponding to the deployment group Gi,j. If the deployment groups are deployed in neighboring locations then the two key-space pools forms a neighbor. After setting the key-space pools, for each sensor node in the deployment group Gi,j, a random set of λ key-spaces is selected from its key-space pool Si,j.

Phase 2: Shared-Key Discovery

This phase differs from the Du-Deng-Han-Varshney (DDHV)-D scheme since Modified Bloom's Scheme is used instead a scheme of the original Bloom's scheme. After deployment, each node tries to find whether it is sharing any key space with its neighbors. Broadcast a message from each node containing the indices of the key spaces it carries. Each neighboring node finds out if there exists a common key space that is shared with the broadcasting node. If such a key space exists, using the Modified Bloom Scheme, the two neighboring nodes derives a pair wise key from the common key space and use those keys to secure the communication links between themselves.

Modified Bloom's Scheme (MBS)

In scheme used to establish secret keys between two nodes which share the key spaces with each other is presented. This scheme is modified for Du-Deng-Han-Varshney (DDHV)-D scheme and the original Bloom's Scheme. So, it is called as the Modified Bloom's Scheme (MBS). In MBS, assume some agreed upon (λ + 1) x N matrix, G, over a finite field GF (q), where, N is the size of the network and q < N. This matrix G is public information and may be shared by different systems, even the adversaries are assumed to know G. During the key generation phase, the base station creates a random (λ x 1) x (λ x 1) asymmetric matrix instead of the symmetric matrix D over GF(q) generated in the original Bloom's scheme and computes an N x (λ + 1) matrix A = (D.G) T . Matrix D should be kept secret and should not be disclosed to adversaries or to any sensor nodes. Since, D is not a symmetric matrix A . G is also not a symmetric matrix. Suppose K = A.G, then the result is Ki,j ≠ Kj,i, where Ki,j and Kj,i are the elements in the ith row and j th column and j th row and i th column of K respectively. To above carry out of the computation, nodes i ,j should be able to compute the Ki,j and Kj,i are respectively. This can be easily achieved by an (MBS)Scheme. The idea is to use key Ki,j to secure the communication link from node i to node j and key Kj,i to secure the communication link from node j to node i. There exists bi-directional links between each pair of nodes which share the key-spaces.

Phase 3: Path Key Establishment

There is a possibility that two neighboring nodes cannot find any common key space between them. In this case, they need to find a secure path to agree upon a common key. It can be observed that two neighboring nodes, i and j, do not share a common key space; but still come up with a secret key between them. The idea is to use the secure links that have already been established in the key-space sharing graph.

V.RESULT AND DISCUSSIONS

Markov Chain Monte Carlo Sampling

MCMC sampling combines the Monte Carlo principle of approximating a distribution by drawing random samples with the principle of Markov Chains. MCMC offers a mathematical framework to ensure that the derived sample has the desired properties. In this setting, the unknown parameters are the states of the Markov Chain, and a proposal function that suggests a new set of parameters based on the current one replaces the transition matrix. The main challenge is to ensure that the Markov Chain and the proposal function fulfill the required properties such that the desired posterior distribution is the invariant distribution of the chain. To this end, various methods existed. One of them is the Metropolis-Hastings algorithm which this research has implemented to protect a WSN from internal attacks. MCMC - MH allows approximating the posterior distribution even if it is not possible to sample from it directly. The following sections discuss MCMC – MH and how does it works in a WSN to find the internal attacker.

Metropolis-Hasting (MH) MCMC adopts the Metropolis-Hasting (MH) to generate a sample from stationary distribution. The objective is to take samples from some distribution π(·) where, π(X)=f(X)/C, where, the C (normalizing constant) may not be known, and very tedious to compute.

Query Dissemination: In the query dissemination phase, the base station broadcasts the aggregation query message throughout the network. The aggregation tree is designed in this phase, if not. μTESLA is used for authenticating the broadcast message.

In the phase of Probabilistic Grouping and Data Aggregation, SDAP randomly groups all the nodes into multiple logical groups and carry out aggregation within each group. Probabilistic grouping is achieved via the selection of the leader node for each group. Because grouping is a dynamic process, a node will not know in advance whether it will become a group leader or which group it will belong to. Sg. While the grouping seed is included in the broadcast query, each node calculates its count value based on the count values received from its children during the aggregation process (as discussed

below). Two functions are used in group leader selection. One is a cryptographically secure pseudo-random function H that uniformly maps the inputs (the node id and Sg) into the range of [0, 1); the other is a grouping function Fg that takes the local node's count value as the input and outputs a real number between [0, 1]. More specifically, each node, say x, decides if it is a leader node by checking whether $H(Sg|x) < Fg(c)$ where c is the count value of node x. If this inequality is true, node x becomes a leader. The function Fg() is constructed such that Fg(c) increases with the count value c. This ensures that nodes with more descendants have a higher probability of becoming group leaders.

Attack-resilient Synopsis Diffusion

The technique of Tree-based aggregation is in danger to communication losses which result from node and transmission failures and are comparatively common in sensor networks. Because each communication failure loses an entire sub tree of readings, a large fraction of sensor readings are potentially not incorporated in the final aggregate at the querying node. The existing protocols, (resilient aggregation scheme and SDAP) resilient to malicious data and remain vulnerable to communication loss. To address this problem, researchers have proposed the use of multi-path routing techniques for forwarding sub-aggregates. For aggregates such as MIN and MAX which are duplicate-insensitive, this approach provides a loss-tolerant solution. COUNT and SUM are the duplicate-sensitive aggregates and double-counting of sensor readings due to the multipath routing, resulting in an erroneous aggregate being computed. Researchers [have presented novel algorithms that solve the double-counting problem associated with multi-path approaches. The Synopsis Diffusion, which is an aggregation framework which is robust and scalable has been proposed for computing aggregates such as COUNT, SUM, UNIFORM SAMPLE and MOST FREQUENT ITEMS.

Synopsis Diffusion, however, does not include any provisions for security, and a compromised node can launch several attacks against this framework which can potentially cause the queried to accept an incorrect result.. These secure protocols are developed by augmenting the original synopsis diffusion algorithms with authentication techniques. Before discussing Roy et al's protocol, we provide an overview of synopsis diffusion, and discuss how a compromised node could launch a falsified sub aggregate attack against the protocol.

To determine the states the nodes observed the traffic feature during the implementation phase (learning phase). This work assumes at the implementation stage WSN is working perfectly with normal traffic, which is the expected traffic from the designed WSN. Hence, each node processes a time series of Æ of such observations. Then the MCMC - MH came into effect to find the acceptance ratio. In the system, this research considers that, if

Table 6.1 Simulation Parameters Performance Metrics

No. of Nodes	30
Are Size	351*351
MAC	802.11
Routing Protocol	DSDV
Simulation Time	50 Sec
Traffic Source	CBR
Packet Size	50bytes
Rate	50Bytes
Transmission Range	150cm
No. of Events	4
No. of Sources	1,2,3 and 4
No. of Attacks	1,2,3,4 and 5
Speed of Events	5m/s
No. of Nodes	30
Are Size	351*351
MAC	802.11
Routing Protocol	DSDV
Simulation Time	50 Sec

the acceptance probability below 60%, the node is said to be an internal attacker. This work set the benchmark for a good node as more than 60% because of WSN characteristics such as signal noise; investigated the Markov Chain Monte Carlo based Metropolis Hasting that has been implemented in WSNs to make decisions about internal attacks. MCMC provides an elegant way to access parameters of a model, even if the corresponding posterior distribution is not accessible. However, In order to implement this method in WSNs, this study does not require training data sets and it works in real time. The simulation results show the acceptance ratio of the internal attacks.

VI. CONCLUSION

The objective of an adversary in the wake of carrying out the node capture attack and various approaches proposed in the journalism to model and detect the node capture is studied. A trusted platform module enabled program integrity verification protocol (TPIV) to detect the node capture attack in a dispersed wireless sensor network setup ensures that only an endorsed verifier can execute the confirmation. Through experimental results it is proved that the protocol does not allow a victim node to elude the confirmation process. The protocol put off a captured node from revealing the secrets of other nodes. With the facilitate verifier sealing the program code of nodes, the protocol does not reveal node program code on verifier compromise. As evident from the performance analysis and experimental results, in comparison to the pure software based protocols, TPIV provides additional security with important reduction

in communication, computation and storage transparency on the nodes. The overall reduced cost of network deployment and preservation is achieved by saving on the cost of having all the nodes enabled. On a successful detection of a node capture assault victim, the victim must be revoked from the network in order to avoid any further smash up to the network. In the next chapter, we discuss a node revocation and key update procedure.

REFERENCES

[1] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy, May 2003, pp. 197–213.

[2] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in ACM Conference on Computer and Communications Security (CCS), 2002, pp. 41–47.

[3] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 2, pp. 228–258, 2005.

[4] O. Ya˘gan and A. M. Makowski, "Zero–one laws for connectivity in random key graphs," IEEE Transactions on Information Theory, vol. 58, no. 5, pp. 2983–2999, May 2012.

[5] O. Ya˘gan, "Performance of the Eschenauer–Gligor key distribution scheme under an on/off channel," IEEE Transactions on Information Theory, vol. 58, no. 6, pp. 3821–3835, June 2012.

[6] R. Di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Connectivity properties of secure wireless sensor networks," in ACM Workshop on Security of Ad hoc and Sensor Networks, 2004, pp. 53–58.

[7] M. Bloznelis, J. Jaworski, and K. Rybarczyk, "Component evolution in a secure wireless sensor network," Networks, vol. 53, pp. 19–26, January 2009.

[8] J. Zhao, "Topological properties of wireless sensor networks under the q- composite key predistribution scheme with unreliable links," IEEE/ACM Transactions on Networking, vol. 25, no. 3, pp. 1789–1802, June 2017.

[9] M. Bloznelis, "Degree and clustering coefficient in sparse random intersection graphs," The Annals of Applied Probability, vol. 23, no. 3, pp. 1254–1289, 2013.

[10] M. Bloznelis and T. Łuczak, "Perfect matchings in random intersection graphs," Acta Mathematica Hungarica, vol. 138, no. 1-2, pp. 15–33, 2013.

[11] F. Gandino, R. Ferrero, and M. Rebaudengo, "A key distribution scheme for mobile wireless sensor networks: q-s-composite," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 34–47, Jan 2017.

[12] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 1, pp. 41–77, 2005.

