Asian Journal of Information Technology 15 (5): 916-920, 2016
ISSN: 1682-3915

A Framework-The Secure Routing and Watchdog System with Multi-Channel Sigryption in Wireless Adhoc Sensor Networks

[1]S. Rajasoundaran, [1]P. Narayanasamy and [2]S. Janakiraman
[1]Department of IST, CEG, Anna University, Chennai, India
[2]Department of Banking Technology, Pondicherry University, Pudhucherry, India

Abstract: Wireless sensor networks are widely applied in rang fields to provide responsive information. The secrecy of the data must be maintained over the open communication medium between the wireless sensor nodes. To provide security for the sensor nodes and the network data, the watchdog sensor nodes have been chosen randomly or hierarchically to detect the adversaries. The previous methods deal with static wireless sensor network to detect the intrusions where the sensor nodes are deployed randomly and don't move anywhere. In Wireless Adhoc Sensor Networks (WASNs), the sensor nodes are always in motion through different transmission regions with various levels of velocities. To select the watchdog sensor nodes or guard nodes in this type of sensor network is really, a challenging task for recent researches. At the same time, here, also the adversaries are moving from one location to another location around the network to do their jobs. To provide flexible security in this Wireless Adhoc Sensor Networks (WASNs), here the secure routing and monitoring protocol has been proposed with multi-variant sigryption using Advanced Encryption Standard (AES) and Digital Signature Authentication (DSA) approach to detect and prevent the moving global adversaries. Based on this approach, the sensor guard nodes are selected randomly and invisibly using complex key management approaches. This will give resilient protection to the Wireless Adhoc Sensor Networks (WASNs) against multiple adhoc adversaries.

Key words: Wireless Adhoc Sensor Networks (WASNs), MDMS, watchdog nodes, sigryption, attackers

INTRODUCTION

Wireless Sensor Networks (WSNs) are the set of sensor nodes collect information from the environmental resources, compute the collected information in to formatted data and communicate with other sensor nodes for finding the path to send that data to the destination through wireless medium. The sensed information can be any stationary or moving objects; pressure and temperature gathered using suitable sensors and processed by the inbuilt microcontrollers of the sensor nodes. Comparing to wired network, these Adhoc sensor Network is more defenseless to protect its sensed data or the task of nodes due to the open channel (Ioannis *et al*., 2007). Any wireless sensor node equipped with sufficient hardware and software can act as an adversary by sensing the wireless channel to grab the transmitting data in unauthorized way. Theses adversaries may try to change the nature the normal sensor nodes and compromise them to do violated activities in the deployed wireless sensor network. This will make the sensor nodes downhill on their performance, throughput and service.

Normally, the wireless sensor network has stable or static nodes that are planted around certain geographical regions to sense and transmit the information. In some cases, sensor network has adhoc sensor nodes where the nodes transit dynamically via different paths to sense the various physical phenomenons. This kind of wireless adhoc sensor network is used to provide valuable communication in the battle fields or defense oriented applications to find out the enemies presence or border violations. Providing security in Wireless Adhoc Sensor Networks (WASNs) is a tough job than SSNs. Because managing the localization of sensor nodes and moving adversaries is the critical one in terms of protection factors. There are different types of attacks created by the adversaries depends on their objectives or without any motives (Ioannis *et al*., 2007; Roman *et al*., 2006).

To detect these kinds of irrelevant activities or attacks, Yun Wang *et al*. (2009) proposes the Intrusion Detection System (IDS) in wireless sensor networks. This IDS is mainly used in wired networks with deployed hardware systems between severs or the nodes to monitor the network activities. Here, the rules are defined for each and every entities involved in that network. The violation of rules by any node is considered as an attack or intrusion will be detected by IDS.

Corresponding Author: S. Rajasoundaran, Department of IST, CEG, Anna University, Chennai, India

Guangcheng Huo and Wang (2008) discusses an approach in Wireless Adhoc Sensor Networks (WASNs). Here, the wireless sensor nodes are presented in distributed manner without any centralized equipments. In this case, this IDS is called as Distributed Intrusion Detection System (DIDS). Based on this DIDS, there are many schemes have been taken to detect the attacks or adversaries in SSNs. One of those schemes is to select watchdogs or monitor nodes to protect the wireless sensor network. Here, the safeguard nodes are selected from neighbor nodes to monitor other nodes to detect the attacks. Those guard nodes are selected in two ways.

Noman *et al* and Yan *et al*. (2009) talks about cluster based scheme. For every session the cluster head is elected as a watchdog which will create computation overhead and causes for single point vulnerability. For Wireless Adhoc Sensor Networks (WASNs), this will not be suitable because of their mobility or random motion (Muhammed *et al*., 2011; Yan *et al*., 2009). In other way, the watchdog nodes have been chosen from nearest neighbors randomly and periodically. The second method doesn't have any steps to ensure the selected node is an adversary or normal node. On both schemes, the selection of safeguard nodes is open in wireless medium without having any security schemes.

Shu *et al*. (2010) discusses the secure data collection via random routes. They proposed multi channel key management approaches. The latest approaches use key management techniques to provide security on the watchdog node selection process which is in sufficient against intelligent adversaries. The adversary with sufficient hardware and software modules of cryptanalysis technique can easily revoke the secret keys and the original data by sensing the unsecured channel.

Crosby *et al*. (2011) provides location based security services to detect and prevent malicious activities. By finding the locations of adhoc sensor nodes, the intelligent attacker can harm the data communication or the nodes'.

Our proposed scheme will provide suitable solution to make concealed distributed watchdog system by selecting and keeping the guard nodes invisible to runtime attackers. This scheme is proposed with the support of symmetric key methods Advanced Encryption Standard (AES). The next sections will give the details about our proposed design and implementations.

Problem definitions and assumptions

Problem statement: In large scale, Wireless Adhoc Sensor Networks (WASNs), n number of sources may send the sensed information as the data packets to m number of receivers at time interval t. There are k number of mobile attackers may move themselves around the entire Adhoc sensor network to sense the open channel or to compromise the sensor nodes. At that time interval t they can inject their attacks like distributed denial of service attack or any runtime attacks to any channel or any node. Here, to compromise the network or node the adversaries are gathering information or any security parameters (keys) from MAC 802.11 data frames by sensing the medium in unauthorized way. To manage this, our proposed scheme will be implemented before MAC 802.11 layer.

Network nature: Let us assume the Wireless Adhoc Sensor Networks (WASNs) with uniform Adhoc sensor nodes having high end microcontrollers, multiple sensing diodes and one or more transceivers according to their needs. The sensor nodes have sufficient hardware modules to handle DES and AES computation and execution process. Among those nodes there are set of adversaries can have their chances to compromise the network with respect to their knowledge and efficiency.

Data communication: The sensed information is converted into collection of bits b_t and transmitted to other sensor nodes with respect to time interval t. In these Wireless Adhoc Sensor Networks (WASNs), the single or multiple senders may transmit their sensed information as the data packets to one or more destinations via multipath data transmission. The optimal forwarding paths will be selected using defined on-demand routing protocol.

Adversary model: There are several Adhoc sensor nodes may acts as an adversaries with necessary hardware and the knowledge about packet data format, data transmission protocols. They may have the facilities to do cryptanalysis process. Those adversaries can change their locations autonomously around the network which will help them to halt or compromise any sensor nodes in the way of performance or data security. This could create severe problem for any nodes to ensure their safety.

Impact of attacks: Here, there are various attacks have been injected from k moving adversaries. Those adversaries can do their attacks of Distributed Denial of Service (DDoS) and Worm Hole (WH). The DDoS has many types of functions like packet dropping, flooding, etc. to stop or reduce the data transmission and reception service between the sensor nodes (Xiao and Chen, 2010). The later one will create the region of compromised sensor nodes (wormhole) to collapse multipath routing process.

Those attacks are injected by the multiple mobile adversaries to damage the RTS/CTS frames in MAC 802.11 layer, RREQ/RREP messages in routing layer and TCP ACKs at transport layer respectively. This causes for loss of data integrity and throughput, increases network overhead and delay. Mainly those attacks focus the open communication channel to sense the exchanging data packets between sensor nodes. To avoid these unauthorized activities of adversaries, our proposed scheme will provide double layered security at the vulnerable layer points. The next section gives the details about our proposed method.

MATERIALS AND METHODS

The Masked Distributed Monitoring Scheme (MDMS): The data packets (P_i, I = 1, 2, 3 ... n) are generated from sensed information at the multiple sources n. The generated data packets are forwarded through optimal data path to several destinations m. Here, the packets are gathered as a collection of bits b(s) and identified as frames in the MAC 802.11 layer. Then those frames are converted into IP fragments at routing layer. In our proposed scheme, we will implement our algorithms at those two layers. By using the Elliptic Curve Cryptography with Digital Signature scheme (ECCDS) and Secure Hashing SHA-1, the set of adhoc sensor watchdogs will be selected randomly at routing layer to inspect the moving adversaries. The Advanced Encryption Standard (AES) and Digital Signature Authentication (DSA) are used to do that elected process invisibly. This will be done by creating black layer between physical layer and MAC 802.11 layer. With this dual protection the masked distributed watchdog system will be developed in adhoc sensor network.

This proposed system has four modules to secure the wireless sensor networks against the attacks. The modules are following: MCDS based Adhoc sensor network design; secure random key management, secure selection of watchdogs-direct approach, secure selection of watchdogs-indirect approach and on demand secured re-routing. This following section illustrates the above modules.

MCDS based Adhoc sensor network design: Minimum Connected Dominating Sets (MCDS) is a graph structure which is used here to connect the nodes to form multiple channels. This approach reduces the link creation overhead with significant level. M(D) is a Minimum

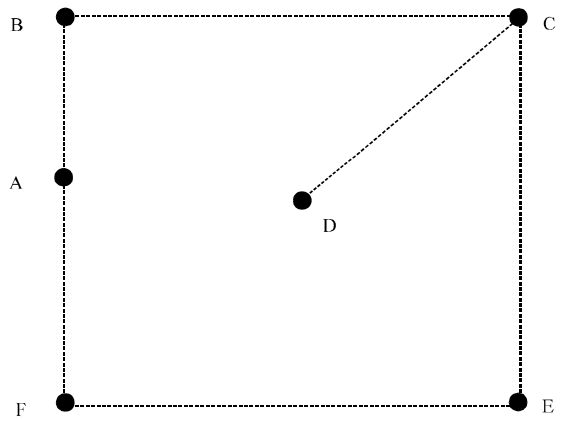

Fig. 1: Minimum connected dominating set

connected dominating set in graph G = (V, E) where V is vertex and E is the edge of the graph. The components of M(D) are called as the dominators.

At a time, one node will dominate others to transmit data. Minimum connected dominating set is a set with minimum possible number of elements among other connected dominating sets. The following fig.1 shows the connections between the vertices and edges.

In Fig. 1 M(D) = {B, C, E} which is connecting the edges and vertices of the graph G with minimal lines. This approach is the adaptable one for large scale Wireless Adhoc Sensor Networks (WASNs) to connect the nodes randomly with minimal cost (Purohit and Sharma, 2010).

Secure random key management approach: Two key generation and management approaches are used to select the watchdog nodes and to re-route the packets at the time of detection of attacks. The first approach is Elliptic Curve Cryptography with Digital Signature scheme (ECCDS) and the second approach is the Secured Hash Algorithm-1 (SHA-1). By these two approaches, the random keys were generated from the defined composite functions to choose the watchdog sensor nodes in safe manner. The next two sections will give the details of the adhoc watchdog sensor nodes selection process.

Secure selection of watchdogs-direct approach: Here, the watchdog sensor nodes are selected form the neighbor nodes which are one hop distance away from monitored nodes. At the same time, the watchdog sensor nodes not selected from the packet forwarding path. To select those nodes, the random key management approach is used which is denoted previously.

The algorithm follows:

K_1= Macid of $P_N \| R_b(P_t)$;
K_s= ECCDS(F_{id} Xor K_1);
F sends K_s to N_1;
N resend K_s to F;
F checks
If (Sent K_s = Received K_s and N_i in $N_I(s)$)
{
N-->W(Watchdog Node)
else
N is an adversary;
}
C_t= OS2IP (SHA1(P_t));Key = H_k;
Source S Send C_t to destination via F;
Destination D decrypt Ct; Get P_t;
F will be monitored by n number of Watchdogs, W
where n = 2
Redo the steps when the sensor nodes moves
from current transmission range to another.

Where, P_t-Plain text; R_b-Random bits; F_{id}-Forwarding node's MAC address; P_N-Preceding node for F; N-Node to be selected as watchdog or not; N_{id} and N_i-MAC address and Index of N respectively; H_k-Hash key; $N_I(s)$-set of indices of sensor nodes.

Here, multiple forwarding nodes may be available between source and destination. They will be monitored by at least three watchdog sensor nodes. The node N which has been selected as a watchdog node will be changed if it does not satisfy the conditions mentioned above.

Secure selection of watchdogs-indirect approach: This approach gives solution to select monitoring sensor nodes at critical situation. In case, any watchdog node is attacked by an attacker or due to excessive traffic in this multipath transmission, we may not have sufficient watchdog nodes (i.e n<2) to supervise the forwarding nodes. At that time, the watchdog nodes are selected from the second or third hop neighbor nodes which are not in the data forwarding path. Before that, the link will be broken with that attacked watchdog node.

The algorithm follows:

K_1 = Macid of $P_N \| R_b$ (P_t)
K_s = ECCDS (F_{id} X or $N_{1\,id}$X or K_1)
F sends K_s to N_1
N_1 send K_s to N_2
N_2 resend K_s to F via N_1
F checks
If (sent K_s = Received K_s and N_{2i} in $N_I(s)$)
{
N_{2i}--> W (Watchdog node)
else
N_{2i} is an adversary
}
C_t= OS2IP (SHA1 (P_t)); Key = H_k
Source S Send C_t to destination via F
Destination D decrypt Ct; Get P_t
F will be monitored by n number of Watchdogs, W
Where n = 3
Redo the steps when the sensor nodes moves from current transmission range to another

Where, P_t-Plain text; R_b-Random bits; N_1-1-Hop node to be selected as watchdog or not; N_2-2-Hop node to be selected as watchdog or not; F_{id} and N_{1id}-Forwarding Node's MAC address and Mac address of N_1 respectively; P_N-Preceding node for F; N_{2id} and N_{2i}-MAC address and Index of N_2 respectively; H_k-Hash Key; $N_I(s)$-Set of Indices of Sensor Nodes.

The watchdog node which has been relived from its function will be automatically changed as forwarding node for some source or an idle one. So, there is no need to keep static sensor watchdog nodes here to provide security against intrusion or an attacker. The selected watchdog nodes will last depends on their mobility, traffic rate and status to be compromised. By selecting multiple random watchdog nodes the wireless sensor nodes could have been secured and the processing overhead of the nodes will be reduced.

RESULTS AND DISCUSSION

On demand secured re-routing: At any time more than two watchdog nodes are available for each forwarding node (channel) to detect the attacker nodes or the attacks. This section provides the details of secured rerouting steps after the watchdog nodes detect the attacks. After the detection of the attacks, there is a need to route the data through secured path. To achieve this, the optimal secured rerouting sources will be selected among the successive watchdog. This will be functioned on demand basis to find the alternate path to precede the multipath data transmission to the original destination. The following algorithm helps to find out the rerouting sources.

The algorithm follows:

F sends R_k to W(s); R_k = ECCDS (R_b X or F_{id} X or W_i);
I = 1, 2, ... n;
W(s) sends RRReq to F; RRReq = R_k X or T_i;
If and only if (Min T_I->W_i);
{
Then W_i is R_N;
}
F sends C_t to R_N
R_N route the packets of C_t to destination

Where R_k-rerouting key; W(s)-Set of watchdogs, W_i-Index of W; RRReq-reroute request; T_I-timestamp, R_N-Rerouting Node. By this approach, there are m number of rerouting sources will be selected for multipath data transmission around the entire wireless sensor network to achieve routing resiliency at the time attack detection. In addition to that the entire selection and routing processes are masked by the black layer using Advanced Encryption Standard (AES) with 128 bit key at different channels as follows,

Sender side

Message encryption:

$$M(F) = E_k(t(m)) \| R_b \quad (1)$$

Signature computation:

$$S(F) = Sig(M(F)) \quad (2)$$

Receiver side

Signature verification:

$$V(F) = Ver_{sig}(S(F)) \quad (3)$$

Message decryption:

$$M_{-1}(F) = D_k(t(m)) \| R_b \quad (4)$$

Where k-AES key, 128 bits; sig-DSA signature key, 2048 bits; Rb-Channel data rate in bits/second. This approach provides significant level of security in routing process and data integrity assurance in adhoc sensor networks.

CONCLUSION

Here, the novel framework for secure routing and watchdog system has been proposed to inspect the data communication sensor nodes and to make secure routing in Wireless Adhoc Sensor Networks (WASNs. These systematic approaches makes the intrusion detection in a feasible manner. Mainly this framework deals with the secure selection mechanisms of watchdog sensor nodes with masked routing conversation using multi channel signcryption. By this, the Adhoc nodes can make their links and communication secure where ever they move at different velocities.

REFERENCES

Crosby, G.V., L. Hester and N. Pissinou, 2011. Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks. Int. J. Network Security, 12: 107-117.

Huo, G. and X. Wang, 2008. DIDS: A dynamic model of intrusion detection system in wireless sensor networks. Proceedings of the International Conference on Information and Automation, June 20-23, 2008, Zhangjiajie, China, pp: 374-378.

Ioannis, K., T. Dimitriou and F.C. Freiling, 2007. Towards intrusion detection in wireless sensor networks. Proceedings of the 13th European Wireless Conference, April, 2007, Paris, France, pp: 1-10.

Mohammed, N., H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, 2011. Mechanism design-based secure leader election model for intrusion detection in MANET. IEEE Trans. Dependable Secure Comput., 8: 89-103.

Purohit, G.N. and U. Sharma, 2010. Constructing minimum connected dominating set: Algorithmic approach. Int. J. Applic. Graph Theory Wireless Ad Hoc Networks Sensor Networks, 2: 59-66.

Roman, R., J. Zhou and J. Lopez, 2006. Applying intrusion detection systems to wireless sensor networks. Consum. Commun. Networking Conf., 1: 640-644.

Shu, T., M. Krunz and S. Liu, 2010. Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE Trans. Mobile Comput., 9: 941-954.

Xiao, Z. and Z. Chen, 2010. A secure routing protocol with intrusion detection for clustering wireless sensor networks. Proceednigs of the International Forum on Information Technology and Applications, Vol. 1, July 16-18, 2010, Kunming, pp: 230-233.

Yan, K.Q., S.C. Wang and C.W. Liu, 2009. A hybrid intrusion detection system of cluster-based wireless sensor networks. Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol. 1, March 18-20, 2009, Hong Kong-.