International Journal of Engineering & Technology, 7 (2.32) (2018) 195-200

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Attack Resistant Agent Based Dynamic Key Management in Dynamic Wireless Sensor Networks

Riaz Shaik[1], Shaik Shakeel Ahamad[2]

[1,2]Department Of CSE, K L E F Vaddeswaram, Guntur District, Andhra Pradesh, India.
CCIS, Majmaah University, Al-Majmaah,Riyadh, Kingdom of Saudi Arabia
**Corresponding author E-mail: sheikriaz@gmail.com*

Abstract

The adaptation of Wireless Sensor Network (WSN) and its utility in real world applications like healthcare is growing faster. With its growth, it also brought vulnerabilities that cause security attacks. It is more so with the emerging technology known as Internet of Things (IoT) which combines physical and digital worlds. At least, as far as WSN is concerned, it is inevitable to have end to end security to protect communications that are sensitive and confidential.Many security schemes came into existence as found in the literature. However, most of them are inefficient for dynamic key management in dynamic WSN. Recently we proposed a scheme named as Agent Based Dynamic Key Management (ABDKM). In this paper we enhance and evaluate it against various attacks such as black hole and rushing.The enhanced scheme is named as an Attack Resilient-Agent Based Dynamic Key Management (AR-ABDKM). The scheme is implemented using NS2. The simulation results showed the remarkable performance improvement of the proposed scheme besides its attack resiliency.

Keywords:*Wireless Sensor Network (WSN), key management, security, dynamic key management system, agent-based key distribution, attack resiliency.*

1. Introduction

Security in WSN has become an important research area as the sensor networks are widely used in the real world. Our work in this paper is an enhanced form of ABDKM [28] to make it attack resilient.When a node drops packets that come on its way without forwarding towards destination, such node is known as black hole and such attack is named black hole attack. The impact of black hole is high when it happens to be a node that connects two components in the network [26]. Rushing attack is when a node wants to establish a route to a destination before actually sending data. Towards this end, RREQ is broadcasted by the sender node to its neighbours. Source node gets information about valid nodes with RREP. Having said this, some protocols exhibit a mechanism known as duplicate suppression which is exploited by attackers to launch an attack known as rushing attack. It is an attack where an RREP is forwarded by attacker on behalf of genuine node with bad intentions. It is done without following proper procedure [27].

Many schemes came into existence in the literature. Many of the schemes are static and developed for static WSN. However, WSN can be dynamic and needs dynamic key management scheme for efficiency. Moreover agent-based key distribution is little explored in WSN. This is the rationale behind the work in this paper. Our scheme presented in [28] is enhanced to make it attack resilient. The proposed scheme is known as AR-ABDKM which is an agent based dynamic key management scheme coupled with attack resiliency. We evaluated the scheme with Two different attacks aforementioned. We made NS2 simulations for proof of the concept. The results revealed better performance of the scheme over other key management schemes.

The remainder of the paper is structured as follows. Section 2 reviews literature on various key management schemes. Section 3 presents the proposed key management scheme named AR-ABDKM. Section 4 presents attack prevention mechanisms. Section 5 provides algorithms to prevent attacks. Section 6 presents experimental results and at the end section 7 gives conclusions and future work.

2. Related Works

This section reviews related works. Kumar *et al*. [1] proposed a key distribution scheme which is based on mobile objects. The concept of the mobile object is to have an object with mobility that moves in pre-defined paths in order to distribute secret keys to nodes in WSN. The scheme showed efficiency in terms of communication and computation besides providing desired security. Cao *et al*. [2] made a review of coordination among agents that work in distributed environment. Distributed agents are used to have coordination in control systems including robotics. Boissier *et al*. [3] explored agent based programming where autonomous agents work in distributed environment to have coordinated efforts to have effective computations. They studied JaCaMo which is one of the multi-agent systems that help in coordinating efforts among distributed systems. Crooks and Heppenstal [4] presented agent based modelling where agents do have characteristics like autonomy, heterogeneity, and active. Object oriented languages are used to have agent based models. Agent based modelling can have more parameters, adaptive nature, aggregation and convenient environment.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wang *et al*. [5] studied multi-agent base model for controlling smart buildings. The model made up of autonomous agents that take care of indoor energy consumption monitoring, comfort, information fusion, aggregation, intelligent controlling and optimization. Blilat *et al*. [6] studied security challenges in WSN that are to be considered while making sensor based systems. Nguyen *et al*. [7] proposed agent based functions into a game theory for controlling smart grids. It was used in renewable energy systems. Fan *et al*. [8] focused on the multi-agent systems and controlling them in distributed environment based on event driven approach. Multi-agent systems are made event-triggered controllers that can help in automating systems where events trigger functionality. Zhao *et al*. [9] on the other hand studied multi-agent systems in terms of finite-time tracking in distributed environments. They followed an observer – based approach for effective control of systems with two communication protocols.

Seyboth *et al*. [10] focused on event-based broadcasting as control strategy in multi-agent distributed system. It is an event based controlling approach with different scenarios. Each agent is modelled based on its intended functionality and local information available. This approach is superior over traditional time-scheduling approach. Sahingoz [19] proposed an agent-based distributed event system that is fault-tolerant. It combined the best features of intelligent mobile agents and event based communication. Nehra and Patel [20] proposed a key establishment mechanism in WSN which is mobile agent based and location-aware. They made use of different kinds of agents for key distribution. They include location calculation agent, set up agent, and key establishment event. Agent manager controls these events as per policies to handle security dynamics in WSN.

Lee *et al*. [13] and Riaz *et al*. [30]studied issues in key management of WSN. They found it to be challenging as it is to be done in resource constrained network. Lu *et al*. [11] focused on key management in cluster based WSN. They proposed two protocols for efficient and secure data transmission n WSN. They evaluated the protocols and found the feasibility of them. Seo *et al*. [12] proposed a key management system for WSN. It was named as Certificate less-Effective Key Management (CL-EKM) with dynamic key management in dynamic sensor network. They found it to be effective in terms of memory, communication and energy consumption. Bechkit *et al*. [14] proposed a scalable key management scheme for WSN. It was based on unital design theory. Ruj *et al*. [15] on the other hand proposed a pairwise and triple key distribution approach in WSN. It is a combinatorial and polynomial approach for secure key distribution.

Gandno *et al*. [16] proposed a static key management system for WSN which supports node addition. It is a random seed key distribution with transitory master key. It also followed pairwise key distribution. Gu *et al*. [17] proposed an end-to-end secure communications mechanism for WSN. It is known as differentiated key pre-distribution. The main feature of this approach is to distribute different number of keys to different nodes in the network. Thus it was able to route information with routes well known for high resiliency against attacks. Traynor *et al*. [18] threw light into combining multiple security approaches for WSN with heterogeneity. It follows probabilistic unbalanced distribution of keys for effective and secure communications.

Sahingoz [21] proposed a multi-level key management system where the key distribution is taken place through a mobile certification authority (MCA) that moves in an aerial vehicle. This key management system was proposed keeping Cyber-Physical Systems (CPSs) in mind. It makes use of symmetric and asymmetric cryptography for effective key distribution and secure communications. Karakehayov *et al*. [22] explored black hole attack and prevention of it by using a system named REWARD. They followed a novel routing mechanism based on geographical routing. It achieves good tradeoffs between life time of network and security. Gondwal and Diwaka [23] proposed detection of black hole attack using an agent in presence of multiple base stations. Baviskar and Patil [24] did similar kind of work in mitigation of black hole attacks. Yet another similar kind of work is found in [25] based on cryptographic primitives. However, there is little research found on agent based key distribution in WSN. We focused on agent based dynamic key management system (ABDKM) in our prior work [28] and this paper is an enhancement it to make it attack resilient. The proposed scheme in this paper is AR-ABDKM which is close to the works in [1], [20] and [21].

3. Proposed Key Management Scheme

We had proposed a dynamic key management system in dynamic WSN in our earlier work [28]. In this we enhanced it and the scheme is labelled as Attack Resilient-Agent Based Dynamic Key Management System (AR-ABDKM). We have enhanced and evaluated meticulously the scheme to make it attack resilient and it is evaluated against the attacks namely black hole attack and and rushing attack. WSN we considered has sensor nodes, base station and cluster heads. Since it is cluster-based, it is optimized for performance improvement. This scheme is agent based. The network model is a typical WSN built using hierarchical topology with multiple clusters. Each cluster is a collection of sensor nodes (SNs). One of the sensor nodes is considered as cluster head (CH). The cluster head of a cluster is able to communicate with other CHs and also base station (BS). BS is the device which high level of resources where data sensed by all sensors is gathered. More details on agent based approach are found in [28][29]. Here we describe the attacks and the prevention mechanisms in the proposed AR-ABDKM scheme.

The below mentioned is the diagram which describes the complete architecture of the attacks , which are considered for the simulation , out of the five attacks represented in the architecture we have implemented two attacks that are

1.Black hole attack
2.Rushing attack

So, this paper particularly addresses the Black hole and Rushing attacks.

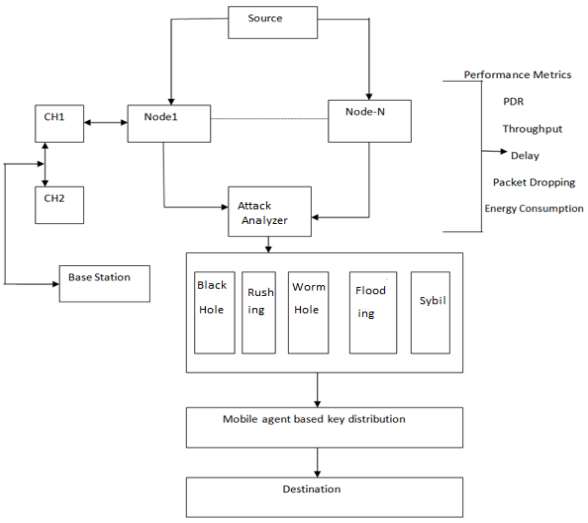


Figure 1: Overview of the architecture

As shown in Figure 1, it is evident that the proposed scheme is a mobile agent based key distribution scheme. It is an extension to our scheme ABDKM [28]. It is enhanced to make it resilient against attacks such as black hole and rushing. It has agent based key distribution mechanism besides mechanisms to handle

security attacks. Particularly, this scheme is evaluated against the aforementioned attacks.

4. Detection Mechanisms for the Attacks

We studied detection mechanisms for the attacks considered in this paper. The details of those mechanisms are found in the following subsections.

4.1. Detection of Black hole Attack

Data is transferred from source to destination through multiple nodes in the middle. In the process the RREQ and RREP (route request and route reply respectively) messages are tracked. DstSeq denotes average difference in each timeslot. This difference between RREQ and DstSeq is computed. Each node involved in the communication records IP address of the destination node besides DstSeq. Feature vector with multiple dimensions is considered to hold the state of each node. The tracking of destination sequence number can help in detecting black hole attack as the sequence number changes as per traffic conditions in normal state. In case of abnormal state, it gets increased abnormally. Modelling and detection of this attack is done as follows.

A three dimensional vector is used to hold the traffic flow in i^{th} time slot. Similar feature space is observed in case of normal state while the abnormal state differs much from it. The mean vector helps in making decisions. It is computed as in

Eq. (1). $\acute{x}^D = \frac{1}{N}\sum_{i=1}^{N} x_i$ (1)

The distance between sample x and mean vector is calculated as in Eq. (2).

$$d(x) = \|x - \acute{x}^D\|^2 \quad (2)$$

A threshold is used to find the occurrence of the attack as in Eq. (3).

$$\begin{cases} d(x) > T_h : attack \\ d(x) \le T_h : normal \end{cases} \quad (3)$$

The threshold value is computed as the projection distance with maximum value. $T_h = d(x_I)$,

Where I= max of d(x_i) (4)

4.2. Detection of Rushing Attack

This attack is detected based on the Bayes' theorem as shown in Eq. (5). When there is no attack associated with a node, S denotes this fact. In the similar way Neg and Pos denote negative and positive probabilities of an attack.

$$P(S \mid Pos) = \left(P(S)P(Pos \mid S)\right) / \left(P(S)P(Pos \mid S) + P\left((\acute{S})P(Pos \mid \acute{S})\right)\right) \quad (5)$$

P(S/ Pos)-> Probability of occurrence of node test is only positive selfishness (Which is attack occurrence). In order to find the selfishness (attack) mutual selfishness with overall selfishness is considered.

$$S = \left(P(S)P(Pos \mid S)\right) / \left(P(S)P(Pos \mid \acute{S})\right) \quad (6)$$

Finally, the probability of attack is computed as in Eq. (7).

$$P(S \mid Pos) = S/(1+S) \quad (7)$$

Regular nodes and not regular nodes are denoted as R and $\acute{R}$ respectively. Here not regular does mean an attack occurred. Prior probabilities such as P(R) and P ($\acute{R}$) are computed using normal density denoted as P(x | R). Network size and node densities are considered in the WSN.

$$P(X/R) = \frac{1}{\sigma_R\sqrt{2\pi}} e^{\frac{-1}{2}\left(\frac{x-\mu_R}{\sigma_R}\right)^2} \wedge P\left(X/\acute{R}\right) = \frac{1}{\sigma_{\acute{R}}\sqrt{2\pi}} e^{\frac{-1}{2}\left(\frac{x-\mu_{\acute{R}}}{\sigma_{\acute{R}}}\right)^2} \quad (8)$$

σ_R, μ_R are notations used to denote summation and detection of an attack respectively. It can be changed as shown in Eq. 9 when continuous variant of Bayes' theorem is used.

$$P(R/X) = \frac{P(R)P\left(\frac{x}{R}\right)}{P(R)P\left(\frac{x}{R}\right) + P(\acute{R})P\left(\frac{x}{\acute{R}}\right)} \quad (9)$$

5. Algorithms Implemented

Based on the study of various attacks, the prevention measures are defined in the form of algorithms. This section provides algorithms implemented to make ABDKM attack resilient.

Algorithm to prevent Black Hole attack

1 Source node broadcasts RREQ
2 Source node receives RREP
3 IF RREP is from the destination or reliable node Then
4 Route Packets to DN
5 ELSE
7 For each **intermediate node** in **all nodes**
8 Send id of intermediate node and further request to next hop node
9 Receive FRp and next hop node of current next hop node
10 Receive data routing info of intermediate node, next hop of next hop node
11 IF next hop node is reliable Then
12 Use data routing info for checking intermediate node for black hole
13 IF intermediate node is not black hole Then
14 Route data packets
15 ELSE
16 Consider it Insecure Route
17 Consider intermediate node as black hole
18 Consider nodes from intermediate node to RREP generator in reverse path as
19 black holes
20 END IF
21 ELSE
22 Current intermediate node = next hop node
23 END IF
24 END IF

Listing 1 – Algorithm to prevent black hole attack

Multiple RREP messages, as shown in Listing 1, for various redundant paths are collected in order to reuse them later when safe route is found. This is to overcome the problems of black hole in the network. Once route request is obtained from source node, the request is observed to know whether it reaches destination. This task is done by reliable nodes. Buffer of data and establishing multiple paths are used to get rid of effects of such attack. Then the route request is rebroadcasted to the same destination. Data transfer among hops is verified and thus black hole is identified. The suspected paths are blocked as to ensure safe routing of data.

Algorithm to prevent Rushing attack

1 Source node broadcasts RREQ

```
2   Source node receives RREP
3   IF node is reliable Then
4   Route data packets
5   ELSE
6   For each Unknown source node
7   Use middle node to send packets to next node
8   Receive reply and routing info of all nodes
9   Validate the route and each node
10  IF data is valid and route is known THEN
11  Route data packets
12  ELSE
13  Suspect rushing attack launched by middle node
14  Fame information is detected
15  END IF
16  IF node need prevention Then
17  Check neighbour node to find node delay
18  Update route with intermediate node
19  Send route information to controller
20  Sender gets route information
21  Discover secure node
22  END IF
23    END IF
24    END FOR
```

Listing 3 – Algorithm to prevent rushing attack

As presented in Listing 3, it is evident that when a node receives RREQ, it is unicasting the request to its neighbour. The RREQ packet is subjected to verification of time interval. The time interval discrepancies are identified and the routing table is updated. Besides suspected operations of the node are stopped. Towards this end, a check request packet is broadcasted. When any packet is obtained from a reliable node, that is fine otherwise an alternative path is chosen. In other words, the node which rushes communication is identified.

6. Experimental Results

We have done simulations with the help of NS2 simulator. NS2 environment is shown in Table 1. The results are captured by NS2 simulations in terms of packet delivery ratio (PDR) vs. simulation time, delay vs. simulation time, throughput vs. simulation time, packet dropping vs. simulation time, and energy consumption vs. simulation time. These metrics can be observed using speed and number of nodes.

Table 1: Shows environment used for simulation

S.No	Parameter Type	Parameter Value
1	Channel Type	Wireless Channel
2	Radio-Propagation	Propagation/TwoRayGround
3	Network Interface	Phy/WirelessPhy
4	Interface Queue Type	DropTail
5	Antenna Model	OmniAntenna
6	Interface Queue Length	50
7	Routing Protocol	AODV
8	No. of Nodes	20, 40, 60, 80, 100, 120
9	MAC type	Mac/802_11
10	Link layer type	LL

As shown in Table 1, the NS environment is used to have simulation study. The results are presented as follows. Routing protocol considered is AODV and interface queue type is DropTail with MAC type IEEE 802.11.

This section provides experimental results based on the simulation time. As simulation time goes on the performance metrics such as packet delivery ratio (PDR), packet drop, energy consumption and throughput are observed and results are presented

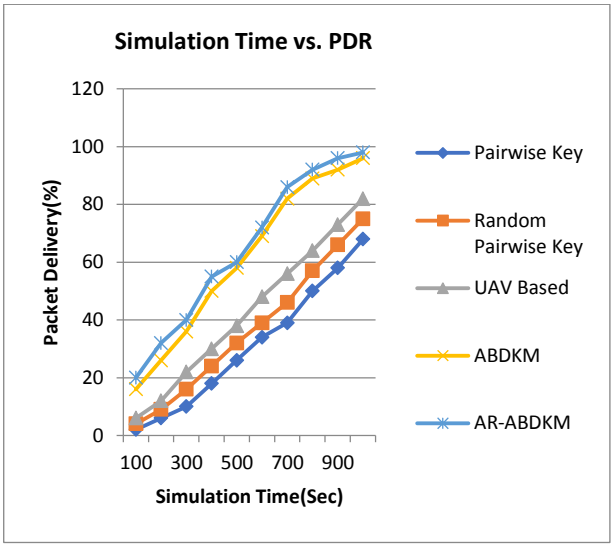


Figure 2: Packet delivery ratio vs. simulation time

In figure 2, X axis shows simulation time and vertical axis shows packet delivery ratio. The proposed scheme AR-ABDKM is showing higher PDR than other schemes. It outperforms all other schemes. The least performance is shown by Pairwise Key while ABDKM is better than all other schemes except AR-ABDKM.

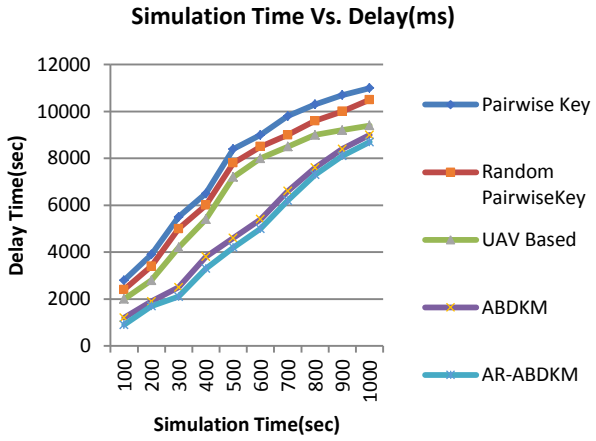


Figure 3: Delay time vs. simulation time

In figure 3, X axis shows simulation time and Y axis shows packet delay time. The proposed scheme AR-ABDKM exhibits least delay time. It outperforms all other schemes. The least performance is shown by Pairwise Key while ABDKM is better than all other schemes except AR-ABDKM. Throughout simulation time, the delay dynamics showed consistent trend for all algorithms.

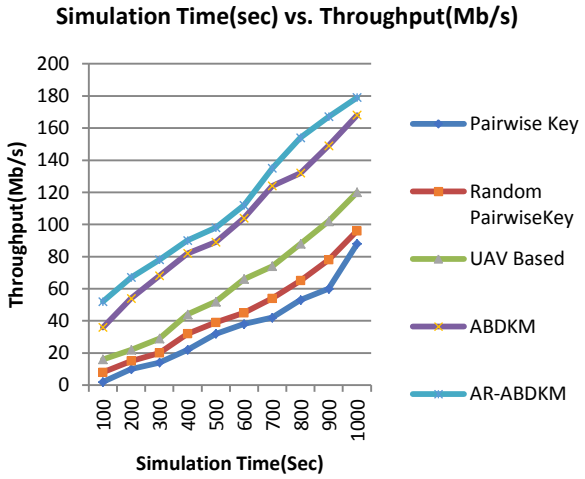


Figure 4: Throughput vs. simulation time

In figure 4, X axis shows simulation time and Y axis shows throughput percentage. Observations are made at different simulation times such as 100 seconds to 1000 seconds by incrementing 100 seconds. The proposed scheme AR-ABDKM exhibits high throughput. It outperforms all other schemes. The least performance is shown by Pairwise Key scheme while ABDKM is better than all other schemes except AR-ABDKM. Throughout simulation time, the throughput dynamics showed consistent trend for all algorithms.

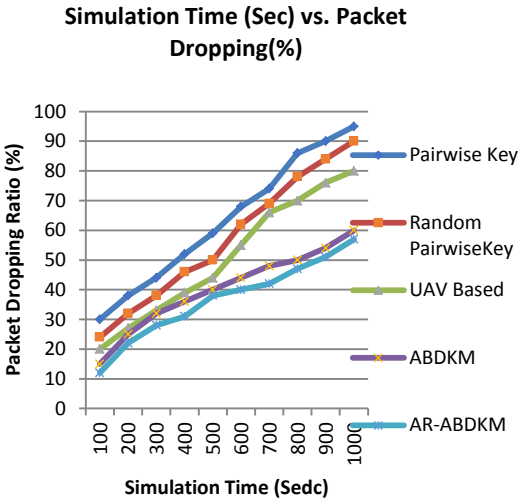


Figure 5: Packet dropping vs. simulation time

In figure 5, X axis shows simulation time and Y axis shows packet dropping ratio. Observations are made at different simulation times such as 100 seconds to 1000 seconds by incrementing 100 seconds. The proposed scheme AR-ABDKM exhibits least packet dropping ratio. It outperforms all other schemes. The least performance is shown by Pairwise Key scheme while ABDKM is better than all other schemes except AR-ABDKM. Throughout simulation time, the packet dropping ratio showed consistent trend for all algorithms.

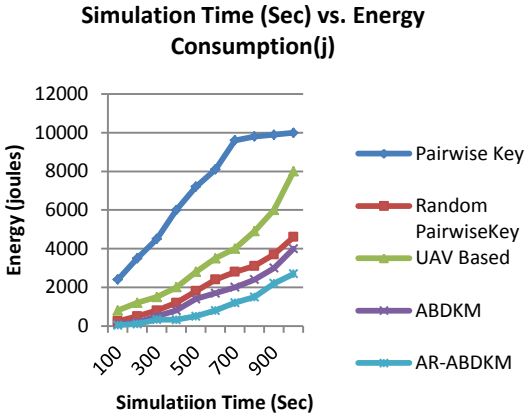


Figure 6: Energy consumption vs. simulation time

In figure 6, X axis shows simulation time and Y axis shows energy consumption. Observations are made at different simulation times such as 100 seconds to 1000 seconds by incrementing 100 seconds. The proposed scheme AR-ABDKM exhibits least energy consumption. It outperforms all other schemes. The least performance is shown by Pairwise Key scheme while ABDKM is better than all other schemes except AR-ABDKM. Throughout simulation time, the energy consumption dynamics showed consistent trend for all algorithms.

The proposed scheme AR-ABDKM is able to secure communications in WSN besides supporting attack resiliency. The scheme is evaluated with different attacks such as worm hole, black hole, flooding, rushing, and Sybil attacks. The results revealed that it has improved performance over other schemes as it is able to withstand attacks and thus exhibits high throughput, least packet drop, least energy consumption and high packet delivery ratio.

7. Conclusions and Future Work

This paper presents a detailed study and implementation of various attacks that may occur in WSN. The attacks we have addressed includes black hole and rushing attacks. Most of the key distribution schemes are either static or used for static WSN. In our prior work, we have proposed an Agent Based Dynamic Key Management (ABDKM) scheme for dynamic WSN. In this paper, we have analysed the scheme with resiliency against aforementioned attacks. The scheme is named as Attack Resilient -Agent Based Dynamic Key Management (AR-ABDKM). This scheme is implemented and evaluated using NS2. The Experimental results proved that the scheme is attack resilient and implements secure communications in WSN. It shows considerable performance improvement over other schemes in terms of packet delivery ratio, packet drop, throughput and energy consumption. In future, we further improve agent based key distribution and evaluate it further.

References

[1] Pardeep Kumar1andPawani Porambage1. (2013). A Mobile Object-based Secret Key Distribution Scheme for Wireless Sensor Networks., p656-660.

[2] Yongcan Cao, Member, IEEE, Wenwu Yu, Member, IEEE, Wei Ren, Member, IEEE, and Guanrong Chen, Fellow and IEEE. (2011). An Overview of Recent Progress in the Study of Distributed Multi-agent Coordination, p1-20.

[3] Olivier Boissiera, Rafael H. Bordinib, Jomi F. H□ubnerc, Alessandro Riccid and Andrea Santid. (2011). Multi-Agent Oriented Programming with JaCaMo. p1-26.

[4] T. Crooks and Alison J. Heppenstall. (2012). Introduction to Agent-Based Modelling,p85-105.

[5] Zhu Wanga, Lingfeng Wang a,?, Anastasios I. Dounis b and Rui Yang a. (2012). Multi-agent control system with information fusion based comfort model for smart buildings. Elsevier, p247-254.
[6] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI LTTI laboratory Sidi Mohamed Ben Abdellah University, FezandMorocco. (2012). Wireless Sensor Network: Security challenges, p68-72.
[7] P. H. Nguyen, Member, IEEE, W. L. Kling, Member, IEEE, and P. F. Ribeiro, Fellow and IEEE. (2013). A Game Theory Strategy to Integrate Distributed Agent-Based Functions in Smart Grids. p568-576.
[8] Yuan Fana,1, Gang Fengb, Yong Wangc and Cheng Songd. (2013). Distributed event-triggered control of multi-agent systems with combinational measurements?. Elsevier, p1-675.
[9] Yu Zhao, Zhisheng Duan, Guanghui Wen and Yanjiao Zhang. (2013). Distributed finite-time tracking control for multi-agent systems: An observer-based approach. Elsevier. 62, p22-28.
[10] Georg S. Seyboth a,1, Dimos V. Dimarogonasb and Karl H. Johansson b. (2013). Event-based broadcasting for multi-agent average consensus. Elsevier, p245-252.
[11] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, FellowandIEEE. (2014). Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks. MICANS INFOTECH. 25 , p750-761.
[12] Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, FellowandIEEE. (2015). Effective Key Management in Dynamic Wireless Sensor Networks. Purdue e-Pubs. 10 , p371-382.
[13] Johnson c. lee and Victor c. m. leung, University of British columbia kirk h. wong, jiannong cao, and henry c. b. chanandhong kong polytechnic university. Key management issues in wireless sensor networks: current proposals and future developments., p76-83.
[14] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh. (2013). A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks 12 , p953-959.
[15] Sushmita Ruj, Member, IEEE, Amiya Nayak, Senior Member, IEEE, and Ivan Stojmenovic, Fellow and IEEE. (2013). Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications.62, p2224-2237.
[16] Filippo Gandino, Member, IEEE, Bartolomeo Montrucchio, Member, IEEE, and Maurizio Rebaudengo, MemberandIEEE. (2014). Key Management for Static Wireless Sensor Networks With Node Adding. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. 10 , p1133-1143.
[17] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan and Xiaole Bai. (2011). Providing End-to-End Secure Communications in Wireless Sensor Networks, p205-218.
[18] Patrick Traynor, Student Member, IEEE, Raju Kumar, Heesook Choi, Student Member, IEEE, Guohong Cao, Senior Member, IEEE, Sencun Zhu, and Thomas La Porta, FellowandIEEE. (2007). Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. IEEE TRANSACTIONS ON MOBILE COMPUTING. 6 , p663-677.
[19] Ozgur Koray Sahingoz. (2007). Agent-based fault tolerant distributed event system.26 , p489-506.
[20] Neeraj Nehra1andR.B.Patel2. (2008). MASLKE: Mobile Agent Based Secure Location Aware Key Establishment in Sensor Networks., p1-6.
[21] Ozgur Koray Sahingoz . (2013). Large scale wireless sensor networks with multi-level dynamic key management scheme. Elsevier, p1-7.
[22] Zdravko Karakehayov,. (2005). Using reward to detect team blackhole attacks in wireless sensor networks. *Computational Sciences and Engineering Division*, p.1-9.
[23] Nitesh Gondwal, Chander Diwaker. (2013). detecting blackhole attack in wsn by check agent using multiple base stations.*American International Journal of Research in Science, Technology, Engineering & Mathematics*, p.345-440.
[24] Ms.B.R.Baviskar,Mr.V.N.Patil. (2014). black hole attacks mitigation and prevention in wireless sensor network.*International Journal of Innovative Research in Advanced Engineering (IJIRAE*. 1 (4), p.123-135.
[25] Ms.B.R.Baviskar, Mr.V.N.Patil. (2014). Black hole Attacks Prevention in Wireless Sensor Network by Multiple Base Station Using of Efficient Data Encryption Algorithms. *International Journal of Advent Research in Computer & Electronics*. 1 (2), p.234-305.
[26] Gulshan Kumar, Mritunjay Rai and Gang-soo Lee "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement" International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012.
[27] L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L. W. Chang. (n.d). Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach (n.d), p1-7.
[28] Riaz Shaik,Shaik Shakeel ahamad (2017). An Agent-Based Hybrid Approach for Dynamic Key Management System in Dynamic Wireless Sensor Network.(JARDCS) journal of advanced research in dynamical and control systems-vol-9,issue-2-OCT-2017.
[29] Riaz Shaik, Shaik Shakeel Ahamad, Enhanced Attack Resistant Agent Based Dynamic Key Management in Dynamic Wireless Sensor Networks. *International Journal of Civil Engineering and Technology*, 8(12), 2017, pp. 69–76.
[30] Riaz Shaik; Shaik Shakeel Ahamad, Key Management Schemes of Wireless Sensor Networks -A Survey. Fronteiras: Journal of Social, Technological and Environmental Science •v.6, n.2, may-august. 2017.