Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

Ensuring Security Using Core Based Routing Algorithm In Wireless Sensor Networks

Azath Mubarakali[1], Dinesh Mavaluru[2]

1 College of Computer Science, King Khalid university, Abha, Saudi Arabia, aabdurrahman@kku.edu.sa, mailmeazath@gmail.com

2 College of Computing and informatics, Saudi Electronic University, d.mavaluru@seu.edu.sa

ABSTRACT

Wireless sensor networks (WSNs) circulate hundreds to thousands of modest miniaturized scale sensor hubs in their locales and these hubs are vital parts of Internet of Things (IoT). In WSN-helped IoT, the hubs are asset obliged from multiple points of view, for example, stockpiling assets, figuring assets, vitality assets, et cetera. Powerful steering conventions are required to keep up a long system lifetime and accomplish higher vitality use. To upgrade WSNs for secured data transmission both at group head and base station data aggregation is required. Data aggregation is performed in each switch while sending data. The life time of sensor arranges lessens in view of utilizing vitality wasteful hubs for data aggregation. Thus aggregation process in WSN ought to be upgraded in vitality proficient way. ESCR will enhance the performance of the system with good potential. Therefore ensuring security using core based routing (ESCR) algorithm in WSNs is proposed. Simulation results show that ESCR perform better than the existing algorithms.

Keywords:

wireless sensor networks, Internet of things, simulation analysis.

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have been used in many applications, like military target tracking & surveillance, wildlife monitoring & natural disaster relief. Communication is a common source of energy ingestion in the WSNs. Hence, the general method is to collectively process the sensor data, yielded by the various sensor nodes while carrying it to the BS. This procedure is known as a data aggregation process. By suing, adding, & filtering the sensor data, the data aggregation process cuts a number of data transmissions & mends the bandwidth energy utilization in WSNs.

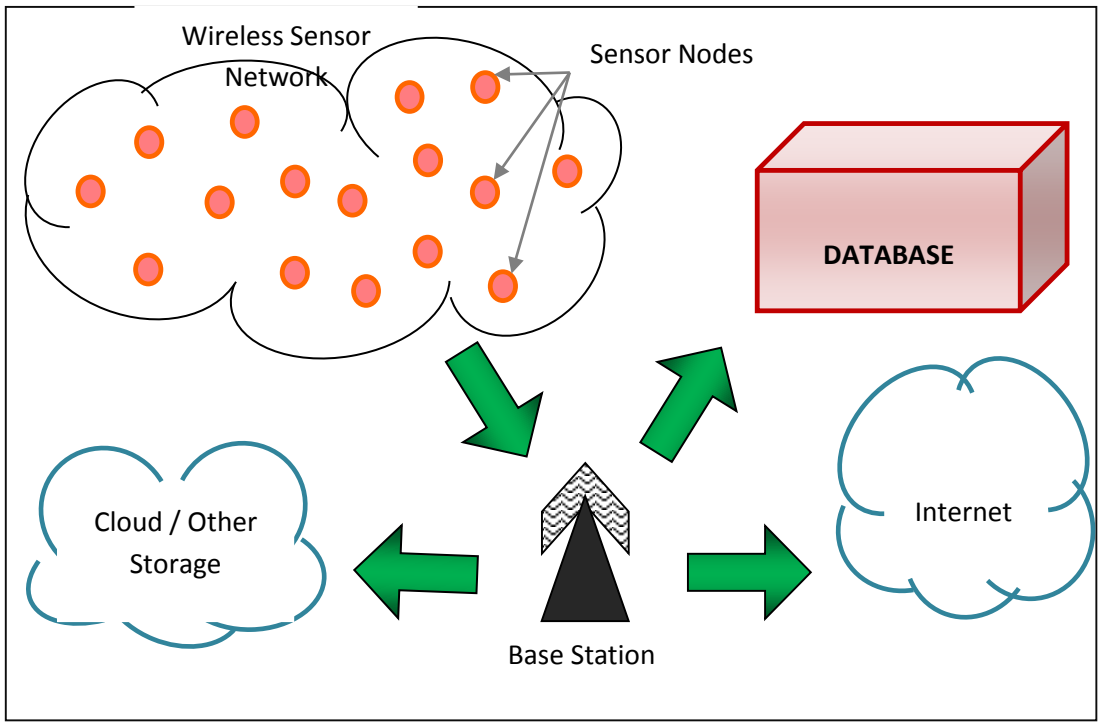

Figure 1: wireless sensor network

A wireless sensor network scenario is shown in figure 1. Various algorithms have been proposed for secure systems those algorithms demonstrate richer robustness equated to the simple averaging methods; however, those algorithms have not been designed by conceiving more sophisticated collusion attack scenarios. Attacker can launch more savvy attacks on the WSNs if they have the idea about the aggregation algorithm and its parameters. They can launch the attack on WSN by exploiting false data injection through a number of compromised nodes.

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

2. RELATED WORK

The synopsis diffusion approach was made secure against the above attack launched by compromised nodes(Alitajer et al, 2016)In particular, an algorithm was enabled to enable the base station to securely compute predicate count or sum even in the presence of such an attack. Clustering algorithms for sensor networks improves network scalability by handling two important problems regarding the size and mobility of the network (Shahbazi,Bemanian,saremi, 2017)

key management schemes plays a critical role in determining the security performance of a WSN network with given application requirements (Bemanian,Shahbazi,2017). To address security issues in the heterogeneous WSNs, a secure clustering scheme along with a deterministic pairwise key management scheme based on public key cryptography was designed (Mahan et al, 2014). In addition, coverage and connectivity to form a single requirement called connected coverage was combined (Bemainan,oryaninejad,shahbazi,2106). The connected coverage is different from requiring non combined coverage and connectivity. Secure data transmission is possible by implementing IF algorithm at the CH [6].

A precise strategy for surveying the reliability of information things was composed and this approach utilizes the information provenance and also their qualities in processing put stock in scores, that is, quantitative measures of dependability [7]. SDAP utilizes a novel probabilistic gathering method to powerfully parcel the hubs in a tree topology into numerous consistent gatherings of comparable sizes. A dedication based jump by-bounce total is performed in each gathering to create a gathering total [8].

A structure where every sensor hub keeps up notoriety measurements which both speak to past conduct of different hubs and are utilized as an intrinsic perspective in foreseeing their future conduct [9]. The initiator computes a session key and a related message in one-pass key establishment protocol [10]. Secured Data Aggregation using Filtering (SDAF) method is compared with the proposed method for analysis.

3. PROPOSED SYSTEM

The WSN has at most N sensor nodes, all the sensor nodes are conveyed in a two-dimensional territory which could be separated into numerous groups. For convenience, the numbers of sensor nodes in the bunch with originating events and the event cell are

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

denoted by Nc and n, individually. According to Nc and n, the network planner can additionally determine the number of mystery shares T to be included in a substantial report and the minimum number of right mystery shares t required to approve a report. Three different types of keys are preloaded as follows:

Firstly, a pairwise key pool is related with a CH utilizing the accompanying system: The measure of the key pool is appropriately set so it is more noteworthy than the quantity of sensor hubs in a bunch Nc. After the arrangement stage, each sensor hub, say, hub u, registers to the CH to let the CH store essential data of the sensor hub. At that point, the CH arbitrarily chooses a pairwise key Ku; CH from the pairwise key pool for the enlisted sensor hub to have a safe correspondence between the CH and the sensor hub. Also, an open/mystery key (PK/SK) match like that assembled is preloaded. The CH signs each message with the SK utilizing an advanced mark scheme and communicates the PK to all the CHs in a similar report validation sending zone for message confirmation. At long last, two mystery keys are shared between the CH and the sink is preloaded to secure the correspondence between them.

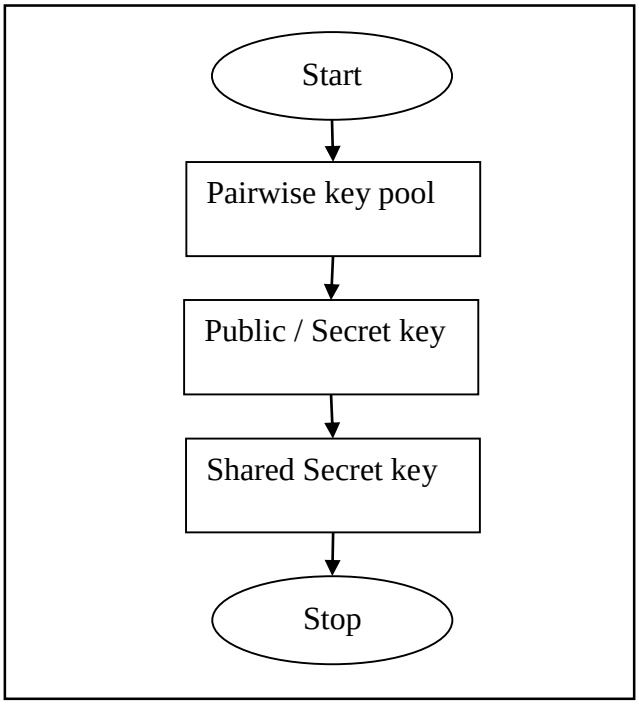

Figure 2: Steps in ESCR

The three important steps for the proposed ESCR in shown in figure 2. Note that T participating sensor hubs concur on the event report S in LEDS and generate secret

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

offers to frame the report to be sent to the sink. The report will be embraced by multiple sensor hubs along the report-authentication sending path. One can without much of a stretch locate the accompanying two disadvantages of LEDS. First, no sensor hub in LEDS is in charge of checking the legitimacy of the report at the earliest reference point of the report lifetime. Therefore, the counterfeit report from an affected cell can travel before it is dropped. In the proposed protocol, each report is first embraced by the CH. Therefore, the counterfeit report is conceivably dropped by the CH. Then again, the CH can check the legitimacy of secret offers. On the off chance that the CH detects any illegitimate secret offer, it will further request a portion of the non-participating sensor hubs to send alternative secret offers.

Once the CH completes information arrangement for report sending, it utilizes computerized signature for marking the message before being sent to the sink. The principle motivation to utilize advanced mark instead of the MAC technique depends on the way that computerized signature dispenses with the likelihood of conferring a fake. Thusly, alternate CHs can confirm the source straightforwardly to stay away from produced signature. Albeit computerized signature ensures that the beneficiaries of the message are free from fabrication or false data, it may cause a message overhead. To limit the message overhead, a great computerized signature scheme ought to be embraced. After accepting the report, the sink confirms the mark and recoups message m. At that point, it checks the freshness of the report with the assistance of the occasion time. Utilizing the property of the sprout channel, all the sensor hubs taking an interest in report age are resolved likewise.

The number of nodes sends the data to the aggregator. The all the nodes have different types of data format. So to aggregate the data that is send to the aggregator node. The aggregator node is also a node that will process the above diagram. Calculate distance of nodes and its trust values. Trusted nodes only send data to cluster head. Based on the information in the packet the nodes trust value is calculated. In this aggregation process the node will sends the data to the aggregator. The aggregator compares the each and energy data. That task is performed by the variance estimator. If the different is more over the data comes for the malicious node. Maximum same data are comes from the goog node. This is not a single time process. It is the iterative process. Based on this approach

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

we can easily identify the trustable nodes by the data aggregation. So this is called secure data aggregation.

4. PERFORMANCE EVALUATION

The performance of the proposed scheme is dissected by utilizing the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete occasion time driven simulator, which is utilized to primarily display the network protocols. The nodes are appropriated in the recreation condition. The simulation parameters are tabulated in Table 1.

The simulation of the proposed scheme has 50 nodes sent in the recreation region 1000×1500. The hubs are moved randomly inside the reenactment zone by utilizing the versatility display Random waypoint. The hubs are spoken with each other by utilizing the correspondence protocol User Datagram Protocol (UDP). The movement is dealt with utilizing the activity display CBR. The radio waves are spread by utilizing the proliferation display two-beam ground. Every one of the hubs gets the flag from all course by utilizing the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay, throughput and residual energy.

Table 1. Simulation Parameters of ESCR

Parameter	**Value**
Number of nodes	50
Routing scheme	ESCR
Traffic model	CBR
Simulation Area	1000x1500
Channel	Wireless Channel
Transmission range	250m
Traffic Model	CBR
Communication Protocol	UDP
Antenna	Omni Antenna

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

5. PACKET DELIVERY RATE

Packet Delivery Rate (PDR) is the ratio of the total number of packets successfully delivered to the total packets sent. It is obtained from the equation 1.

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \tag{1}$$

Figure 3 shows the PDR of the proposed scheme ESCR is higher than the PDR of the existing method SDAF. The greater value of PDR means better performance of the protocol.

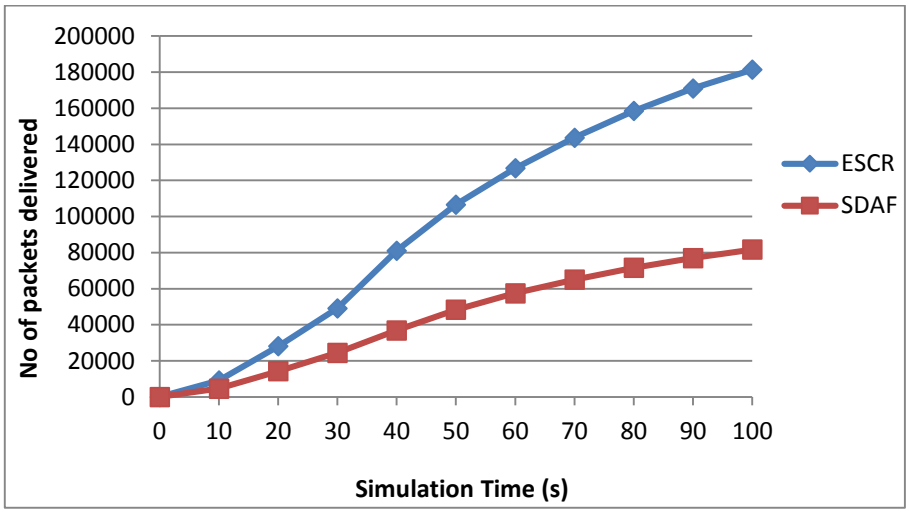

Figure 3: Packet Received Rate

6. AVERAGE DELAY

Average Delay is defined as the time difference between the current packets received and the previous packet received. Average delay is obtained from equation 2.

$$Delay = \frac{\sum_{0}^{n} Pkt\ \mathrm{Re}cvd\ Time - Pkt\ Send\ Time}{n} \tag{2}$$

Where n is the number of nodes.

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

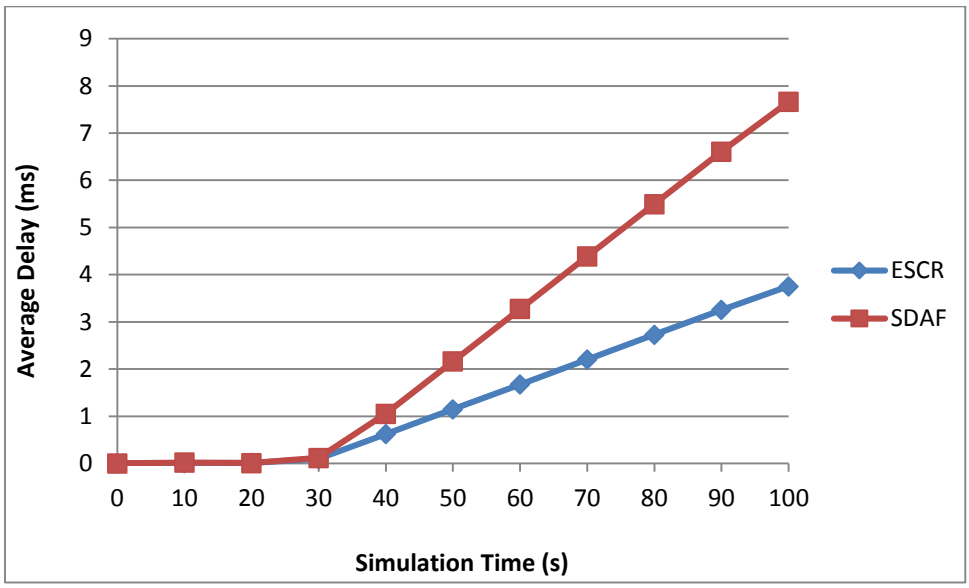

Figure 4: Average Delay

Figure 4 shows that the delay value is low for the proposed scheme ESCR than the existing scheme SDAF. The minimum value of delay means that higher value of the throughput of the network.

7. RESIDUAL ENERGY

The energy that remains in a node at the current time is called as residual energy.

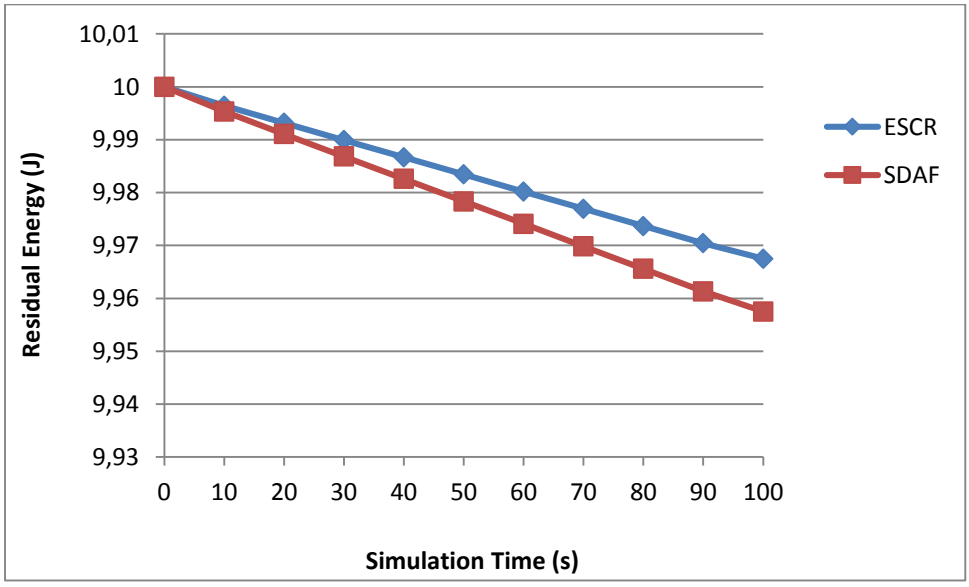

Figure 5: Residual Energy

Figure 5 shows that the residual energy for the ESCR scheme lasts longer when compared with the existing scheme SDAF.

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

8. CONCLUSION

Ensuring security using centroid based routing (ESCR) algorithm in WSNs is proposed in this paper. Data aggregation is performed in every router while forwarding data. The life time of sensor network reduces because of employing energy inefficient nodes for data aggregation. Hence aggregation process in WSN should be optimized in energy efficient manner. ESCR will enhance the performance of the system with good potential. Simulation analysis also shows the improved performance of this core based routing approach.

REFERENCES

Shahbazi, Mehrdad, Mohammad Reza Bemanian, and Hamid Reza Saremi. "Analysis of Effective Key Factors in Adaptability of a Building in the Future with an Emphasis on Flexibility in Historical Buildings (Case Study: Bu-Ali of Hamadan)." *Space Ontology International Journal* 6.1 (2017): 69-78.

ALITAJER, S., SAJADZADEH, H., SAADATIVAGHAR, P., & SHAHBAZI, M. (2016). The Role of Physical Factors in the Sociopetalness of Informal Settlements: The Case of Hesar-e Emam and Dizaj Neighborhoods in Hamedan.

Mahan, A., Bazvandi, F., Shahbazi, M., & Bazvand, K. N. (2014). Evaluation of Compatibility of Architectural Styles in Change of Use in Historical Buildings Case Study: The Study of Change of Use in Tabriz Leather Factory to Islamic Art University

Bemanian, Mohammadreza, Reza Oryaninejad, and Mehrdad Shahbazi. "Typology of spatial expansion new sprawl pattern (Case study: Urumia urban region)." Journal of Turism Hospitality Research 5.4 (2016): 65-80.

BEMANIAN, MOHAMMAD REZA, and MEHRDAD SHAHBAZI. "FUNCTIONAL ROLE IN THE VITALITY OF URBAN OPEN SPACES (CASE STUDY: ERAM PARK HAMADAN)." (2017): 57-68..

Roy, S., Conti, M., Setia, S., & Jajodia, S. (2014). Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact. IEEE Transactions on Information Forensics and Security, 9(4), 681-694.

Received 17/04/2018
Approved 10/06/2018

Pradeepa, K., Anne, W. R., & Duraisamy, S. (2012). Design and implementation issues of clustering in wireless sensor networks. International Journal of Computer Applications, 47(11).

Alcaraz, C., Lopez, J., Roman, R., & Chen, H. H. (2012). Selecting key management schemes for WSN applications. Computers & Security, 31(8), 956-966.

Azarderskhsh, R., & Reyhani-Masoleh, A. (2011). Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2011(1), 893592.

Dietrich, I., & Dressler, F. (2009). On the lifetime of wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 5(1), 5.

Padmaja, P., Marutheswar, G. V., & Niharika, K. S. (2016). Optimization Of Wireless Sensor Networks In Secured Data Aggregation. International Journal of Electrical and Electronis Engineering Research, 7(2), 94-100.

Lim, H. S., Moon, Y. S., & Bertino, E. (2010, September). Provenance-based trustworthiness assessment in sensor networks. In Proceedings of the Seventh International Workshop on Data Management for Sensor Networks (pp. 2-7). ACM.

Yang, Y., Wang, X., Zhu, S., & Cao, G. (2008). SDAP: A secure hop-by-hop data aggregation protocol for sensor networks. ACM Transactions on Information and System Security (TISSEC), 11(4), 18.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(3), 15.

Mishra, M. R., Kar, J., & Majhi, B. (2014, May). One-pass authenticated key establishment protocol on bilinear pairings for wireless sensor networks. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on (pp. 1-7). IEEE.

Received 17/04/2018
Approved 10/06/2018

Revista Publicando, 5 No 15. (2). 2018, 1051-1061. ISSN 1390-9304

Acknowledgement:

I (Dr Azath Mubarakali) would like to thank king Khalid university for the infrastructure and environment was provided to lead this paper, we thank our colleagues who provided insight and expertise that greatly assisted the research. We would also like to show our gratitude to for sharing their pearls of wisdom with us during this research, and we thank "anonymous" reviewers for their so-called insights.

I (Dr Dinesh Mavaluru) would also like to show my gratitude to the Saudi Electronic University for allowing me to do research and for sharing their pearls of wisdom with us during this research, and we thank reviewers for their so-called insights. We are also immensely grateful to people who supported this research and for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

Received 17/04/2018
Approved 10/06/2018