International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 6 –OCTOBER 2016 (SPECIAL ISSUE).

Avoiding Collusion Attack in Aggregation of Data for Wireless Sensor Network by Pre-Key Distribution Technique

Rahul[1], Jayashree Agarkhed[2]

Professor, Dept of computer science and engineering, PDACEG, Kalaburgi, India
P.G Student, Dept of computer science and engineering, PDACEG, Kalaburgi, India

Abstract—**Wireless sensor network (WSN) nodes have less energy and computation power so aggregation of data from multiple sensor network is done through a technique called averaging, which is more vulnerable to nodes compromising attacks . Iterative filtering algorithm is more robust against collusion attacks than simple averaging methods. But this will not take care of false data injection and sophisticated attacks so we apply pre-key distribution to each node which authenticate with base station to aggregate the data by avoiding attacks.**

Index Terms—Aggregation, collusion attack, iterative filtering algorithm, pre-key distribution.

I. INTRODUCTION

WSN consists nodes that sense the data, process data and communicate with each other. Technology has made it possible to have very small, low powered sensing devices equipped with programmable compute, multiple parameter sensing and wireless message capability. Low cost of sensor nodes to have a network of hundreds or thousands of these sensors, thereby improving the consistency and accuracy of data and the area coverage. WSN provide information about isolated structures, wide-spread environmental changes, etc. Wireless sensor nodes to monitor physical or environmental situation, such as sound, temperature, and motion

WSN have limited computational power and energy resources. Averaging is simple method used to aggregate data from multiple sensor nodes. This method of aggregation is known to be highly vulnerable to node compromising attacks. Since WSN are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks. So trustworthiness of data and reputation of sensor nodes is crucial for WSN. Performance of very low power processors improves; future aggregator nodes will be capable of performing more sophisticated data aggregation algorithms to make WSN less vulnerable. Iterative filtering algorithm holds great promise for such a purpose. Iterative filtering algorithms provide aggregation data from multiple sources nodes and provide trust assessment of these sources, usually it is done by assigning weight factor to each sensor node.. We demonstrate that several existing iterative filtering algorithms, while significantly more robust against collusion attacks than the simple averaging methods, are nevertheless susceptive to a novel sophisticated collusion attack we introduce to address this security issue, we propose a modified iterative filtering techniques by providing an initial approximation for such algorithms which makes collusion robust, but also more accurate and faster converging.But this technique will not find more sophisticated collusion attack.To overcome from this problem we introduce technique that is by assigning a pre-key distribution to each sensor network,the sensor network verify the key with the base station if the key match is found then aggregation of data is done from source to the destination .

The proposed work is improving the trust of the sensor network by making pre-key distribution which will ever come the limitations of the WSN that is that are false data injection and more sophisticated collusion attack

II. RELATED WORK

The author [1] the data aggregation is done through simple method called averaging. This is vulnerable to many kind of attacks.

The authors [2] considered a problem of many kinds of attacks so to avoid those kind of attacks we used a iterative filtering algorithm to aggregate the data which improves trust of the sensor nodes

The author [3] Iterative filtering algorithm didn't hold a great promise for sophisticated collusion attacks so the algorithm is improved by assigning a intial weight factors to sensor nodes which improves the trust of sensor nodes

The authors [4], The pre-key distribution to the sensor nodes is done which helps in aggregation of data this technique is vulnerable to many kind of attack .If false data intruder can find the key the data can be used.

From the literature survey it is found that iterative filtering algorithm will not hold great promise to more sophesticated collusion attacks and false data injection and also the pre-key distribution will not avoid the attacks .

The proposed method improves the trust of the sensor nodes by applying a pre-key distribution technique to the

wiresless sensor network which are already made trustworthy by applying iterative filtering algorithm.

III. PROPOSED WORK

Aggregation of data is done using keys. In this every sensor node sense the data which needs to be aggregated at the aggregator point. So we need to increase the trust of the each sensor node.

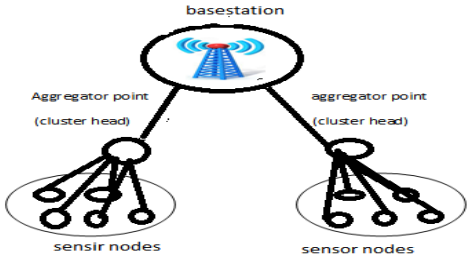

Fig 1. Model of WSN

Fig 1 shows the set of sensor nodes which sense the data the data needs to be aggregated at the aggregator point. Base station will help in aggregation of data. Base station will contain set of keys for each sensor node so the sensor node request base station before sending data to destination if the key of the sensor network matches the keys of the base station if the match is found then we transfer the data to the destination .

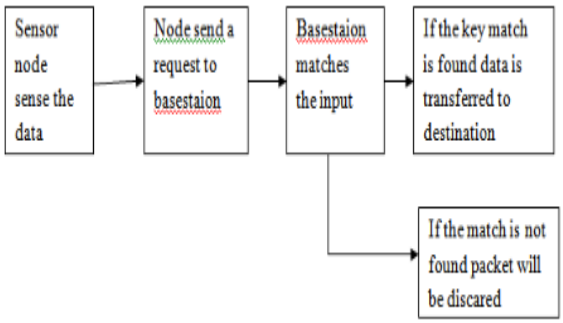

Fig 2. Block diagram of data transfer

The Fig 2 shows the verification of input data of the sensor node. Sensor node need to aggregate the data so before sending the data to aggregator point it verify the key match with the base station will be containing setting of keys of the nodes. If the key is found in the base station then it send the response message to particular node to send the data to aggregator point. If the key is found in the base station packet will be discarded.

If any collusion attack is happening in the path of data transmission it is identified and data transmission will choose a different path rather than choosing collusion attack path. Trust of the sensor nodes is important concern in WSN .By making use of this key technique we will improve the sensor network so that efficiency of data transmission will improve. Energy consumption of the sensor node can be decreased. It will detect false data intruder if the key match is not found. attacker may be present in the path base station verify its key then match will not be found then it will detect the attacker .since the energy of the sensor network is low attackers are present in the path data transmission will not happen efficiently.

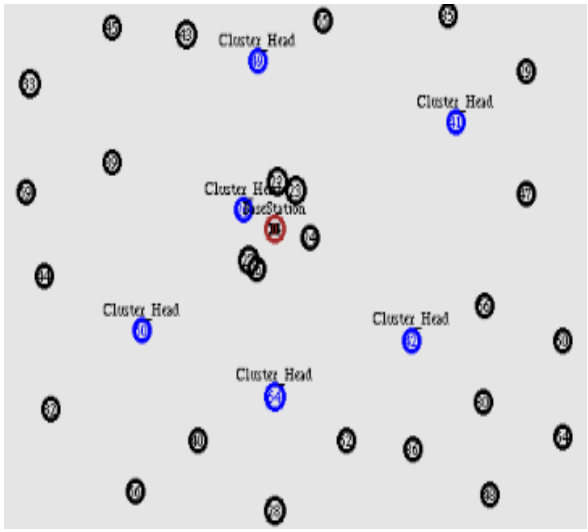

Fig 3. Structure of the network

The node with the highest energy is choosen as a cluster head in this it is the the node which is ready to transmit the data to the aggregator point is chosen as a cluster head diagram shows the cluster heads and base station from where the data is needs to be requested.

Base station will contain all the keys which need to be maintained securely. Each and every node will go and verify with the base station so the communication of data will happen faster and performance of the system will increase because each node will verify before transferring data to the aggregator node. Matching of each key will take time to verify but the aggregation of data will happen securely. Energy of the node will go down once the data is transferred. The node which is ready to send the data which is choosen as a source node. The source will contain the highest energy will be ready to transfer the data.

This technique will reduce the delay and energy consumption because of node DSDV routing protocol is used for routing. Which will help in identify the path of attack. Due to this data transmission will choose efficient path to transmit the data to the aggregator point.

Source input node needs to aggregate data to the destination node. There are many kinds of attack will happen which are identified. False data intruder try to acces the data from the network that is identified by the basestaion. The attck is found due key mismatch in the basestaion. Other simple averaging and iterative filtering algorithm will technique will not take care of all these sophisticated and false data intruder attacks.

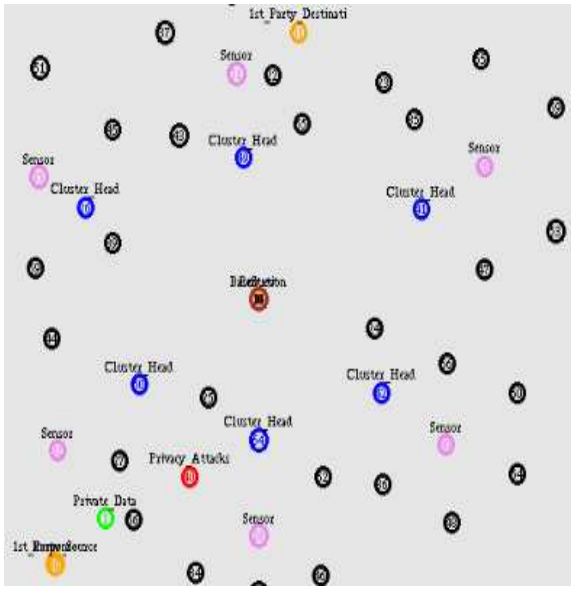

Fig 4. Detection of attack in the network

Fig 4 shows the data transfer from source to destination where the input data need to be aggregated data transfer will happen by matching of the key with base station .In the path there are many false data intruder are present which will request the base station. Key mismatch will happen in base station then its identified as a attack as shown in the in the figure by doing this we can avoid collusion in the path of data transfer. Trust and reputation of the wireless sensor nodes is the very important concern in WSN. It's improved by doing by pre-key distribution rather than doing other technique.

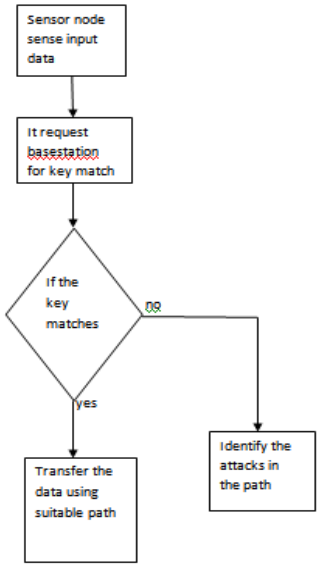

Fig 5. Flow chart for data transfer by identifying attack

Fig 5 shows that complete data transfer and identifying attacks by making use of key matching parameter.If the mismatch is found because of false data injection.It identify the path in which the attck is happening which will help in avoiding such path by this we can avoid collusion.

IV. RESULT ANALYSIS

A simulation model based on NS2 is used, assumed that the dimension of the scenario as 300x300m in that 70 wireless node randomly deployed. Each wireless nodes initials energy is 10joules, 10 Mbps bandwidth and each packet size 512 kbps. A two way propagation model is assumed by radio model

SIMULATION PARAMETERS

Parameter	Setup
set Val (Chan)	Channel/Wireless Channel
set Val(prop)	Propagation/Two Ray Ground
set Val(net if)	Wireless Physical
set Val(Mac)	Mac/802_11
set Val(if q)	Queue/Drop Tail/Pri Queue
set Val(LL)	LL
set Val(ant)	Antenna/Omni Antenna
set queue length	30
set Val(num nodes)	70
set Val(routing protocol)	DSDV
set Val(x)	2000
set Val(y)	1000
set Val(stop)	350

Table 1.simulation parameters

.

V. PERFORMANCE ANALYSIS

In this section, the evaluation of the proposed work is carried out. The observations for security, energy efficiency and packet delivery ratio of the proposed work are noted and graphs are plotted.

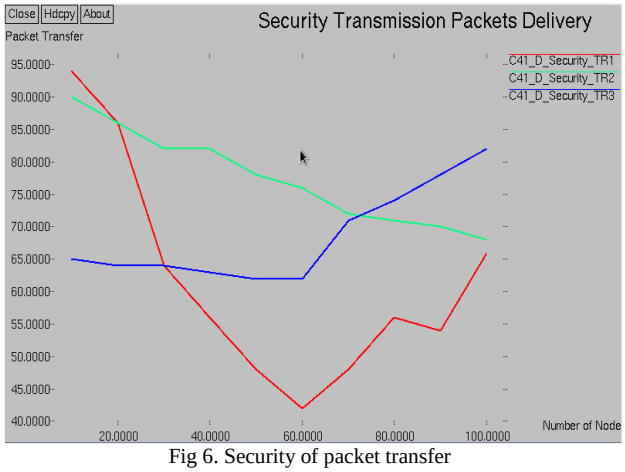

Fig 6. Security of packet transfer

Fig 6. shows security of packet transfer rate for methods.The red line indicates simple averaging technique in that packet transmission will decrease due its more vulnerable to many kinds of collusion attacks so to over another method is used i.e. iterative filtering algorithm which provides better

security compared to simple averaging technique so the green line in graph shows better security compared to red one. Still iterative filtering algorithm will not take care of more sophisticated collusion attack. So in the graph the blue line indicates pre-key distribution method which provides better security than iterative filtering algorithm .proposed system provides better security than previous methods.

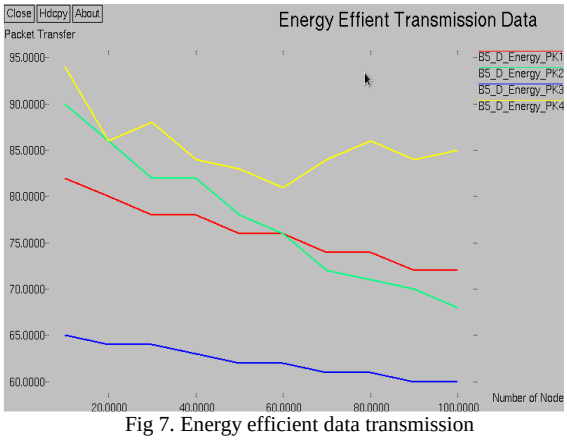

Fig 7. Energy efficient data transmission

Fig 7. shows the energy efficient packet transfer. The yellow indicates data transfer that is in simple averaging technique is constant with respect to energy efficient transfer. Green lines of the graph indicate iterative filtering algorithm in that the graph is constantly decreasing which indicates its not energy efficient transmission. Red lines of the graph indicates modified iterative filtering algorithm which is also decreasing so its not energy efficient. Blue line indicates our proposed work that is constant compared to other so pre-key distribution technique is better energy efficient compared to existing techniques.

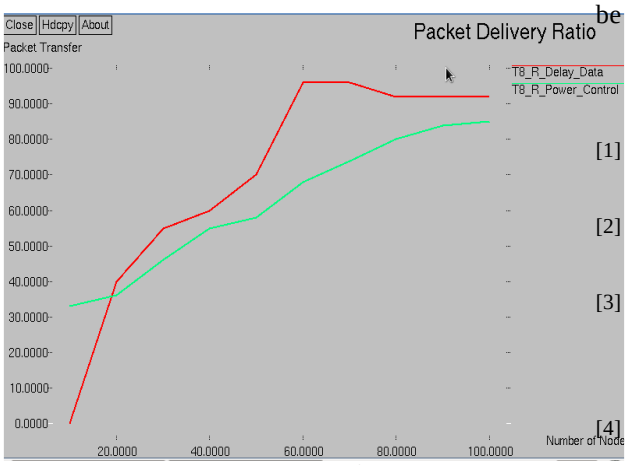

Fig 8. Packet delivery ratio of proposed work

Fig 8. Shows the delay and power control ratio of the of the proposed work the red line indicates delay exist in the system when the number of packet increases base station needs to authenticate each keys so delay will increase. Green line indicates the power of sensor node if the number of the nodes power control ratio also should be more

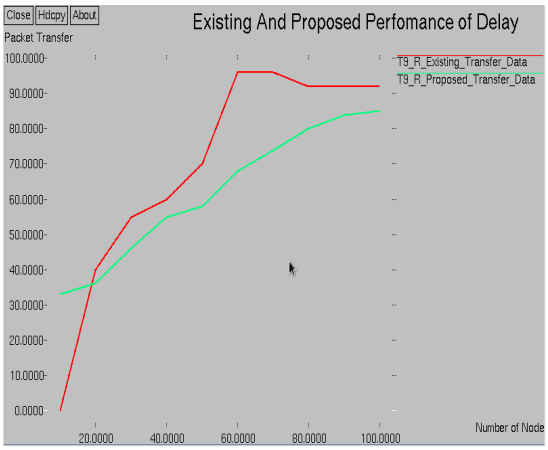

Fig 9. Comparision of performance

Fig 9. shows the proposed system is better than the existing system the green line indicates the proposed system in that the graph that is the number of packet transfer will increase with the number of nodes increases. This increasing of graph is cinstant as shown in fif where as red line indicates fluctuation of packet transfer when the number of nodes increases this fluctuation is due to collusion attacks

VI. CONCLUSION

Several technique have been used to aggregate data in WSN that are simple averaing technique, iterative filtering algorithm technique but these will not take care of sophisticated collusion attacks. so to overcome from this we make use of technique called pre-key distribution which will avoid these kind of attack due to which performance and security of the WSN increases. Trust and reputation is important conern for WSN.our proposed system provide better security so trust and reputation of the sensor node will be increased.

REFERENCES

[1] S. Ozdemir and Y. Xiao, “Secure data aggregation in wireless sensor networks: A comprehensive overview,” Comput. Netw., vol. 53, no. 12, pp. 2022–2037, Aug. 2009.

[2] C. de Kerchove and P. Van Dooren, “Iterative filtering in reputation systems,” SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

[3] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha, “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks” IEEE transactions on dependable and secure computing, vol. 12, no. 1, january/february 2015

[4] Firdous Kausar1, Sajid Hussain2, Jong Hyuk Park3, and Ashraf Masood1 ashrafm61, Nova Scotia, , A Key Distribution Scheme Preventing Collusion Attacks in Ubiquitous Heterogeneous Sensor Networks.

[5] Y.-K. Yu, Y.-C. Zhang, P. Laureti and L. Moret "Decoding information from noisy, redundant, and intentionally distorted sources", *Physica A: Statist. Mech. Appl.*, vol. 371, pp.732 -744 2006

[6] P. Laureti, L. Moret, Y.-C. Zhang and Y.-K. Yu "Information filtering via iterative refinement", *Europhys. Lett.*, vol. 75, pp.1006 -1012 2006

[7] Y. Zhou, T. Lei and T. Zhou "A robust ranking algorithm to spamming", *Europhys. Lett.*, vol. 94, p. 48002, 2011 C. de Kerchove

and P. Van Dooren "Iterative filtering in reputation systems", SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp.1812 -1834 2010

[8] C. de Kerchove and P. Van Dooren "Iterative filtering in reputation systems", SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp.1812 -1834 2010

[9] Eli Biham. New types of cryptanalytic attacks using related keys. J. Cryptology, 7(4):229{246, 1994.

[10] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In EURO- CRYPT'05, volume 3494 of LNCS, pages 507525. Springer, 2005.

[11] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256, 2009, available at http://eprint.iacr.org/2009/317.pdf.