World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-4, Issue-5, May 2017 Pages 21-25

Approaches for Excluding Compromised Node by Evaluating Trust in Wireless Sensor Network

Ravneet Kaur, Priyanka Mehta

***Abstract*—This paper analyse the most important and significant advancements in wireless sensor network using AES key encryption sign for identification. Wireless Sensor Network (WSN) is a collection of sensor nodes that involve in gathering of happenings from a nodes' surrounding. Routing attacks are one of the most common attacks in which the attacker can make disorders in wireless sensor network communications. In order to confronting these attacks, encryption methods are not enough because compromised node, have access to the secret information and can go across the traditional methods. At this time, the most effective way to confront these attacks in WSNs is to use trust management systems. Different trust systems have been proposed to reduce the effect of routing attacks, but most of them could not determine the malicious node effectively and some of them suffer from the attacks on the system. In this paper, we propose a centralized trust management system using authorization and encryption and exclude compromised node by evaluating the trust factor in wireless sensor network, which is not only resistant against routing attacks but also against the trust system attacks.**

***Index Terms*— Networks, Authorization, Encryption, Cryptography, Authentication etc.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of geographically distributed nodes, where nodes are small size battery driven devices deployed over hostile areas. The sensor nodes are connected with each other in Ad-hoc manner, the devices have capability of running various applications and communicating with other nodes within the network and each node transmits its sensing information to a Sink node which collects all the data as a whole from various other nodes after that the total collected measured aggregated data then reach the various applications through a gateway. The sensor nodes can participate in transmitting data to the other nodes within its predefined range.

As the wireless sensor network infrastructure is infrastructure less thus some unique topologies of the network enables dynamic adjustment of the individual nodes in a hostile area. WSN is considered as a most prominent and efficient networking technology as so many nodes have CPU power and radio transceiver capacity and can be deployed over a sensing area where most of the conventional networks with fixed infrastructure are insufficient to perform a particular task.

As the power source of each node has some limited capacity so the efficient and the throughput of the network is also limited. Various external factors such as weather conditions can affect the performance of the wireless sensor network. Wireless sensor network is already in use of environmental monitoring, habitat monitoring, and defense etc. All the communication within the wireless sensor networks (WSN) are specialized transducers with spatially dispersed and dedicated autonomous sensor nodes for identifying, monitoring and recording the physical and environmental conditions at different locations.

WSN is a revolutionary technology that comprises of several sensor nodes that are small in size, light in weigh and easily portable. These sensor nodes are laced with a radio transceiver, a microcontroller and a battery, which can either be embedded in it or located externally as an energy resource. The function of the radio transceiver is to connect the sensor nodes or neighbor nodes with an external link while the microcontroller is an electronic circuit that plays a significant role to interface the sensor nodes thereby forming a complete circuit to effectively process, store, receive and send data to the base station.

The security of Wireless Sensor Network (WSN) is under grave threat due to the attacks on the sensor nodes, which are often categorized as goal-oriented attacks, performer-oriented attacks and layer-oriented attacks. This type of attack is called passive attack which results in the revelation of sensitive information to the attacker without any knowledge at the user's part. However, in the active attack, the attacker actively assesses the entire network to gain control over it. The best and most common ways of active attack includes data modification, spoofing, sinkhole, flooding, jamming the network, warm hole, black hole, fabrication, lack of co-ordination, node subversion, false nodes, selective forwarding and so on. While in performer-oriented attacks, the attacks are either internal or external. Internal attackers are the trickiest ones as they are not only the legitimate node of the original network but also have direct access to all the sensitive network information. The internal attacks include modification, misrouting, eavesdropping and packet dropping attacks that leads to suppression of critical information reaching the base station, thereby degrading the network performance.

II. PROPOSED WORK

The main Emphasis of our research is on to check the trust factor of node from centralized server i.e Cluster head which control the whole network to prevent the problem of black node.In this, according energy consumption and trust value,we will make the cluster head using highest energy and

Ravneet Kaur, Department of Computer Engineering ,Universal Campus, Lalru (SAS Nagar), Punjab, India
Priyanka Mehta , Department of Computer Engineering ,Universal Campus, Lalru (SAS Nagar), Punjab, India

higher trust value. The node that have lowest enrgy and lower trust value, Base station will send an encrypted message to That particular node and, user will decrypt the message, if the decrypted message matched to original message then Base station automatically increase the trust value otherwise,it will declared as Compromised Node and Base station will exclude this node from the network.For preventing the black node we have following rules to build up the wireless Sensor Network

A. Authentication phase:

For fresh node, there will be two phases to join the network:: in authentication phase server will check some unique parameters If all parameters are matched then authentication is done and server will send a encrypted message to Client.

B. Excluding Phase:

In authorization phase user will decrypt the message received by server using its key and send to the server, if decrypted message is matched with the sending message then authorization phase is done and user will be logged in. For communication there will be key agreement phase between two users, so by this black node will be unable to communicate into the network. we make cluster head with the help of energy and with highest trust value that will check every node trust factor and exclude all the black nodes. File sharing will be using encryption method so that if black users receive this file will be unable to decrypt this file.

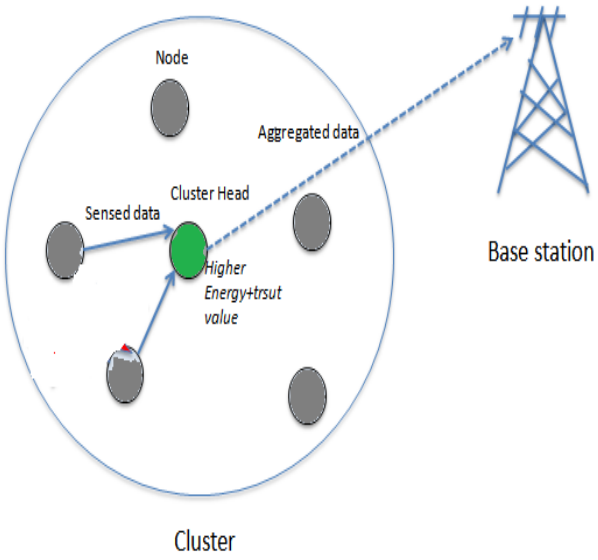

Fig 1: Distribution of Cluster Head in Multiple Nodes

III. IMPLEMENTATION

A. Registration Phase:

In registration phase server will give Big Integer unique key, ID to user.

Example: client1, client1, 911 4567950

Username→client1,password→

client1,userkey→911,ID→4567950

B. LoginPhase:

Login phase is following divided into two parts:--

a) Authentication phase:

In authentication phase server will check the following parameters:
1.Macaddress
2.Username
3.Password
4.Unique Key
If all parameters are matched then authentication is done and server will send a encrypted message to user using AES algorithm.
AES Algorithm steps:
1. First select the string to be Encrypted.
2.Select the cipher mode if Encryption: select Cipher.ENCRYPT_MODE
3. Get the String content into Bytes
4. Encode this bytes Using Base 64 Encoder
5. Now encrypt the final result With the help of AES algorithm.
b) Authorization Phase:

In authorization phase user will decrypt the message received by server using its key and send to the server, if decrypted message is matched with the sending message then authorization phase is done and user will be logged in.

Algorithm:

1. First select the file to be decrypted.
2. Use key for Decrypt the file
3. Select the cipher mode if Decryption: select Cipher.DECRYPT_MODE
4. Now Decrypt the Final Result with the help of AES algorithm.
5. Get the file content into Bytes.
6. Decode this bytes Using Base 64 Decoder

C. File Sharing:

When user wants to share the file, firstly key agreement phase will be placed, key agreement phase is done using IBE algorithm.

Algorithm steps:

Firstly, user requests to server for receiver's Id ,public key and a no.

a) User will encrypt the message using receiver's id, public key, and a no. will get from the server.

b) Receiver will decrypt this challenge using its private key, no, user id got from server.

If receiver decrypted message matches with sender message then, file sharing is possible between them.

ENCRYPTION:

On the server file will be encrypted, using RSA with homomorphic + AES algorithm,

Steps:

1. Apply Homomorphic with RSA algorithm : The homomorphic property is that multiplication is preserved.

C(x1)â‹…C(x2)=(xe1modm)â‹…(xe2modm)

2. Now using encrypted key, the AES algorithm applies as:
1. First select the file to be Encrypted

2. Use key for Encrypt the file
3.Select the cipher mode if Encryption: select Cipher.ENCRYPT_MODE
4. Get the file content into Bytes
5. Encode this bytes Using Base 64 Encoder
6. Now Encrypt the Final Result with the Help of AES algorithm

Example: firstly server selects master key for the particular user and apply Rsa Homomorphism on it as:

1. Using master key Homomorphic will generate two numbers i.e p,q--This returns a BigInteger of bitLength bits that is probably prime.

For Example,

P=357 and q=337

Compute n = p * q = 257 * 337 = 86609

(p-1)*(q-1)=256*336=86016

Now we have to chose an exponent, e that is relatively prime to $\phi(n) = (p-1) * (q-1)$. The pair (e, n) is our public keythat is used to encrypt messages.

e=17

Public Key and private key Generation:

Pub=17,86609

Pri=65777,86609

Now using RSA the following encryption is applies using public key:

The encryption of $c = m^e \mod n$

C=1244812334565456

Returns Digital Signature i.e Used as key (1244812334565456)

Key (1244812334565456) in hexadecimal is→31 32 34 34 38 31 32 33 33 34 35 36 35 34 35 36

Suppose now we have text to be encrypted as:" Wireless sensor"

Change it to Hexadecimal code :57 69 72 65 6c 65 73 73 20 20 73 65 6e 73 6f 72

Perform X-OR operation on it with key and Pass this cipher text as plain text into AES as:

In order to increase the throughput 4 rows are divided in to1 row.

D. *Download file:*

For download file user requests to server and if user is authenticated then server send all the file data to the user.

E. *Decrypt File:*

At the time of decrypting file, the request goes to server and if user is authenticated then server send encrypted key to the user, and user will decrypt message using this key using following algorithm:

1. First select the file to be Decrypted
2. Use key For Decrypt the file
3. Select the cipher mode if Decryption: select Cipher.DECRYPT_MODE
4. Now decrypt the final result with the help of AES algorithm
5. Get the file content into Bytes
6. Decode this bytes Using Base 64 Decoder

IV. RESULTS & DISCUSSION

A. *Aggregation Accuracy*

In wireless sensor networks (WSNs), data aggregation schemes have been extensively investigated in order to reduce energy, although it has a great side-effect, the end to end delay is increased. In this proposed structure, each layer of clusters has specific delay and accuracy in order to aggregate the information within a given time and predetermined accuracy level. Data aggregation is an essential technique to reduce the communication overhead and prolong network lifetime.

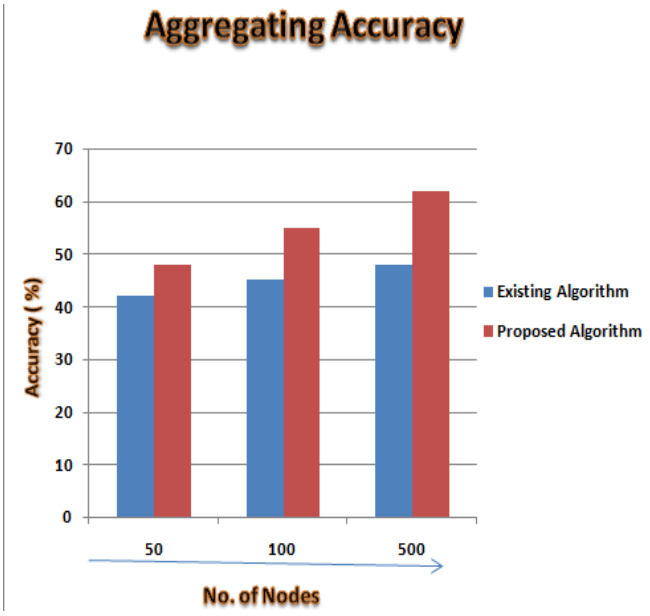

Fig 2

Table 1

No. of Nodes	Existing Algorithm	Proposed Algorithm
50	42%	48%
100	45%	55%
500	48%	62%

B. *Energy Consumption:*

Energy consumption is the core issue in wireless sensor networks (WSN). To generate a node energy model that can accurately reveal the energy consumption of sensor nodes is an extremely important part of protocol development, system design and performance evaluation in WSNs

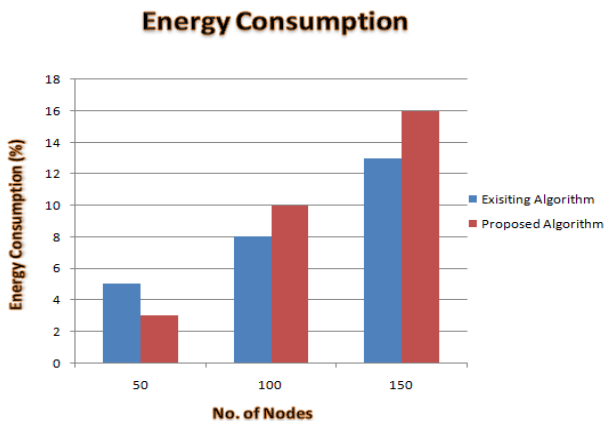

Fig 2

Table 2

No. of Nodes	Existing Algorithm	Proposed Algorithm
50	5%	3%
100	8%	10%
500	13%	16%

C. Trust Value:

A wireless sensor network (WSN) is a collection of distributed sensor nodes to work together for monitoring the physical and environmental conditions. Trust in wireless sensor networks is an important issue and it solves the problem of access control, privacy, secure routing scheme and reliable communication. The multiple versions of a trust state / recommendation of the target node is received at the trust requestor. The aggregation operation must be performed at the trust requester in order to obtain a single trust value for the target node. Trust requester must ensure about the trusted path in which the recommendations / opinions are forwarded.

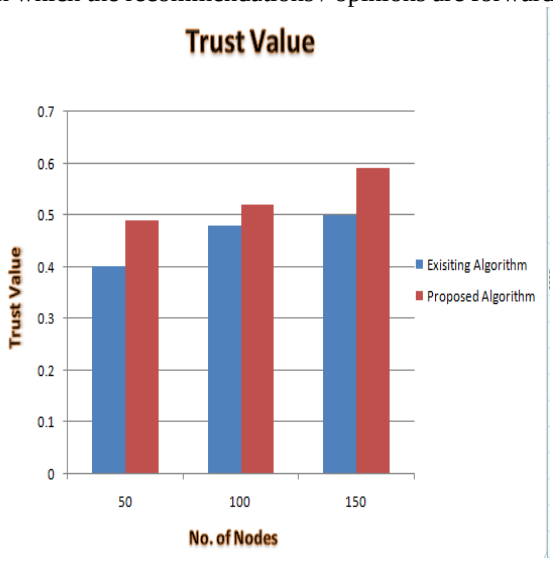

Fig 3

Table 3

No. of Nodes	Existing Algorithm	Proposed Algorithm
50	0.4	0.49
100	0.48	0.52
500	0.5	0.59

D. Compromised Value:

A node on which an attacker has gained control after network deployment. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

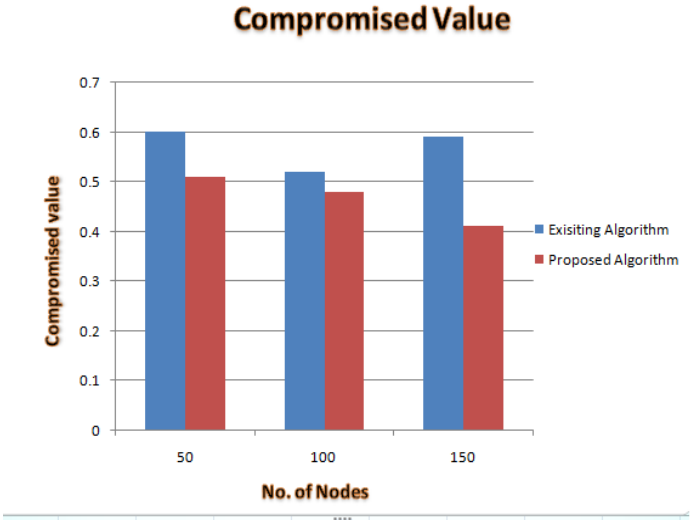

Fig 4

Table 4

No. of Nodes	Existing Algorithm	Proposed Algorithm
50	0.6	0.51
100	0.52	0.48
500	0.5	0.41

V. CONCLUSION

There are multiple trust and reputation techniques available to detect the selfish and malicious nodes. The basic methodologies for trust techniques and various research work under each category been addressed. Sensor applications has wide range of applications and each applications been addressed and security can be addressed and implemented in each application. We suggest for future work to provide an efficient algorithm with less pattern can be easily taken from any surface that the person touches. It is also considered that fingerprints and footprints are the most popular evidences in the places of crime. In a day and age of consumption of energy, power and memory techniques are addressed and no compromise on the security strength is made. Self learning algorithms based on scoring system framework may be implemented further for improving their liability of the systems, which would have advantages in terms of learning new data patterns if there is a change and thus able to identify

the change fast as time changes even if the probability of factors influencing the trust factor changes due to change in scenario.

REFERENCES

[1] Jun-Won Ho, Wright .M, S.K. Das, "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," IEEE Transactions on Dependable and Secure Computing, Vol. 9, no. 4, pp. 494 - 511, July/August 2012.

[2] T. Abuhmed, N. Nyamaa, and D. Nyang, "Software-Based Remote Code Attestation in Wireless Sensor Network," Proc.IEEE GLOBECOM, Dec. 2009.

[3] T. Park and K.G. Shin, "Soft Tamper-Proofing via Program Integrity Ver-ification in Wireless Sensor Networks," IEEE Trans.Mobile Computing, vol. 4, no. 3, pp. 297-309, May/June 2005.

[4] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT:SoftWare-Based Attestation for Embedded Devices," Proc. IEEE Symp. Security and Privacy (S& P), May 2004.

[5] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed Software-Based Attestation for Node Compromise Detection in Sensor Networks," Proc. IEEE 26th Int'l Symp. Reliable Distributed Systems (SRDS), Oct. 2007.

[6] Mathews .M, Min Song, Shetty .S, McKenzie .R "Detecting Compromised Nodes in Wireless Sensor Networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Vol .1, pp. 273-278 August 2007.

[7] Bose, P. Morin, I. Stojmenovic, J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks", *ACM Wireless Networks*, vol. 7, no. 6, pp. 609-616, 2001.

[8] A. Dahbura, K. Sabnani, L. King, "The comparison approach to multiprocessor fault diagnosis", *IEEE Trans. on Computers*, vol. C-36, no. 3, pp. 373-378, 1987.

[9] J. Deng, R. Han, S. Mishra, "Security support for in-network processing in wireless sensor networks", *2003 ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03)*, 2003.

[10] J. Deng, R. Han, S. Mishra, "A Robust and Light-Weight Routing Mechanism for Wireless Sensor Networks", *Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS)*, 2004.

[11] W. Du, J. Deng, Y.S. Han, P. K. Varshney, "A Witness-Based Approach For Data Fusion Assurance In Wireless Sensor Networks", *IEEE 2003 Global Communications Conference (GLOBECOM)*, 2003.

[12] W. Du, J. Deng, Y.S. Han, P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks", *10th ACM Conference on Computer and Communications Security'03)*, 2003.

[13] Michael L., Simon A.C., Ruth M., Kathleen J., "Truth Machine: The Contentious History of DNA Fingerprinting", University of Chicago Press: Chicago, (2008)

[14] Soni N., Siddiqua A., " Filtering Techniques used for Blurred Images in Fingerprint Recognition", International Journal of Scientific and Research Publications (ISSN 2250-3153), Vol. 3 (Issue 5), May 2013 .

[15] Amrita Ghosal and Jyoti Prakash Singh "Secure Data AggregationUsing Some Degree of Persistent Authentication in Sensor Networks"Proceedings of the Conference on Mobile and Pervasive Computing (CoMPC-2008), pp. 183-186, August 2008.

[16] Aravind Iyer, Sunil S. Kulkarni, Vivek Mhatre and Catherine P.Rosenberg "A Taxonomy-Based Approach to Design of Large-Scale Sensor Networks", proceedings of the Conference on Wireless SensorNetworks and Applications, Signals and Communication Technology,pp. 3-30, 2008.

[17] Banerjee, I., Chanak, P., Sikdar, B.K. and Rahaman, H. "EER:Energy Efficient Routing in Wireless Sensor Networks", Proceedings of the IEEE Students' Technology Symposium (TechSym) pp. 92-97,Jan 2011.

[18] Algorithms",Proceedings of the IEEE Workshop on High PerformanceSwitching and Routing (HPSR'04), Phoenix, pp. 241-245, April 2004.