IJRSETAPRIL 2017 Volume 4, Issue 4 Pages: 61-68
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

ESD-WSN: - ENHANCED ENERGY EFFICIENT AND SECURITY BASED DATA DISSEMINATION IN WIRELESS SENSOR NETWORKS

[1] R.Rajareka ,[2]M.Sathya,
[1,2] Assistant Professor,
[1]Computer Application Department, [2]Computer Science Department
[1,2]T.K.S.College of Arts and Science, India.

ABSTRACT: In our proposed frame work, use hybrid techniques are clustering scheme and Security management for improve network life time and security In this paper, we propose and evaluate an energy efficient clustering scheme for periodical data gathering applications in WSNs. In the cluster head election phase, a constant number of candidate nodes are elected and compete for cluster header nodes to the node remaining power. This work is determined and without steps, thus it has much lower message overhead. The method also produces a near uniform distribution of cluster heads. And this cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. In our proposed security framework we using Random Key Pre-distribution .RKP schemes have several variants. Their system works by distributing a key ring to each participating node in the sensor network before deployment. We propose a key management scheme that relies on probabilistic key sharing among nodes within the sensor network.

Keywords: [Wireless Sensor Networks, Energy efficient Clustering Scheme, Security Key Management.]

1 .INTRODUCTION

In Wireless networks, the grouping framework is a secure manner in obtaining high power, so the model of high power grouping framework for WSN is very important. In WSNs the sensor nodes are power controlled. Therefore, it is main work to prevent some ideas to give more flexible and more amount of energy efficiency to prolong network lifetime. One solution is by clustering network nodes into sets called clusters. Grouping gets more latency of the sensor network by breaking the sensor network into groups of sensors to conserve communication energy. At last, saving the power and improving the whole latency of the topology is obtained. Adopting clustering scheme produces two-level hierarchy; the upper level and the bottom level. The upper level is arranged by the nodes that are response for collecting and fusing the received data from sensor nodes in the sensing area and then transmit it to a central controller; such nodes are named the Cluster Head (CH) nodes. The bottom level of the hierarchy is formed by the nodes that are responsible for detecting the required data from the sensing range and then forwarding it to the responsible CH. All clusters include no of sensor nodes and one cluster head (CH). CH selection can be centralized performed by the BS or the last user based on some process. It can also be broadcast in formal and worked by the sensors themselves on a localized level. The BS is responsible for processing data received from network sensing nodes to be processed by the last user. This work, we used a new broadcasting energy efficient cluster head selection algorithm in which two factors are incorporated: the sensors' residual energy levels and the distances between sensors and the CH.

In this process the framework of random key pre-distribution to address the bootstrapping problem. First, we propose the random key pre-distribution scheme, which achieves greatly strengthened authentication by small range malicious while reduced improving security in the face of a large scale physical attack on network nodes. We will explain why this trade-off is a desirable one. And then, we use the multiple route secure process, which substantially improves the security of key setup such that an attacker has to communicate various nodes to get a more probability of communicating any given transmission. Finally, we propose the random-pair-wise keys scheme, which assures that, even when some number of nodes have been compromised, the recall of the network recalls fully authenticate. And also, this process maintains hop-by-hop security management between neighbors and quorum-based node revocation without involving a Sink node. Hop-by-hop security management it obtains to the range that any node can ascertain the identity of the nodes that it is communicating with.

2. PROPOSED MODEL

2. 1 DSR Protocol

Overview and Main functions of the framework The DSR protocol is connected of double process that work at the same time to permit the determine and performance of client path in the centralized network: Route Discovery is the process by which a node S wishing to transmit a data to a destination node D contains a source path to D. Route Discovery is used only when S attempts to transmit a data to D and does not earlier know a path to D. 3 Route Maintenance is the process by which node S is able to detect, while using a source path to D, if the network range has changed such that it can no more use its path to D because a link along the path no longer works. When Route Maintenance indicates a source path is block, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route.

Path determine and Path performance each process fully on demand. In particular, unlike other frameworks, DSR requires no timely data of any kind at any step within the network. For example, DSR does not use any timely path ad, link status sensing, or nearby detect packets, and does not rely on these functions from any underlying protocols in the network. This fully depended function and lack of timely process allows the number of high data caused by DSR to scale all the way down to zero, when all nodes are not accurately stationary with regards to each other and all path needed for current transmission have already been discovered.

As nodes start to mobility more or as transmission patterns change, the routing data highly improve of DSR automatically scales to only that needed to track the routes currently in use. In response to a one Route Discovery (as well as through path information from other data higher), a node may read and cache more paths to any destination. This permits the reaction to routing changes to be much more rapid, since a node with more routes to a destination can try another cached path if the one it has been using should fail. This caching of more than routes also omits the overhead of needing to perform a new Route Discovery each time a path in use breaks to various antenna or propagation patterns or sources of interference.

2.2 Clustering Scheme

Clustering is a useful function for decreasing power usage in wireless sensor networks (WSN). To get a good network latency performance, various grouping mechanism use different metrics for cluster head (CH) election. For example, the sensors own remaining energy as well as the network's total residual energy is used. In this paper, we use energy aware grouping that use both the residual energy levels of sensors within a group radius as well as the degree. To achieve this, we define a metric that is scale at each sensor based on intra information within its nearby node. This metric is incorporated within the CH election probability. Using these parameters, one can select the sensors with less residual energy amount to have the better impact on CH election which results in CH election being biased to be near to these sensors. This results in decreasing their transmission energy rate to the CH.In this mechanism, the grouping protocol is a main function in get power efficiency, so the design of an energy-efficient grouping algorithm for WSN is more important. In WSNs the sensor nodes are energy constrained. Therefore, it is most particular to find some solutions to offer more scalability and satisfy more energy efficiency to prolong network lifetime. One solution is by clustering sensor nodes into sets named clusters. Clustering achieves good lifetime of the sensor network by interrupt the sensor network into clusters of sensors to conserve transmission energy.

Process steps:

For ; : maximum number of rounds
For , is the index for sensor node
Find set(sensors in cluster radius)
Calculate weight
Calculate cluster weight
Perform CH selection
Inform all sensor nodes in the cluster
Cluster formation will begin
End of current round condition
Restart new round condition

In network the sensor nodes are often grouped into separate disjoint sets named a cluster, grouping is used in WSNs, as it gives network scalability, resource distributes and most use of constrained resources that gives network range stability and energy saving parameters. Clustering techniques decrease transmission overheads, and efficient resource allocations thus reducing the whole energy usage and decreasing the interferences between sensor nodes.

A more number of groups will traffic the range with less size groups and a very small number of groups will select the group head with high rate of data transmitted from group members. Proposed technique is hierarchical routing based on grouping and find the best number of groups in WSNs in order to save energy and optimize network lifetime. In this process, we have surveyed the state-of-art of grouping algorithms in WSNs.

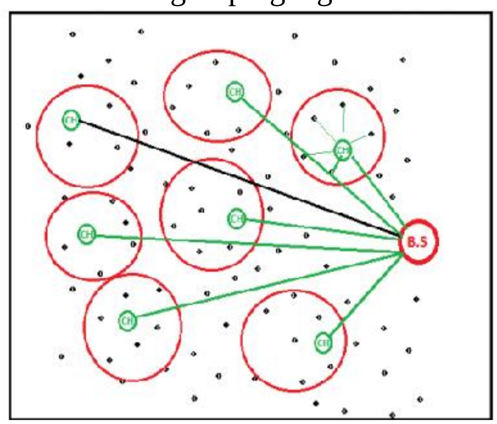


Figure 1- Cluster Creation

2.3 Random Key Pre Distribution

Basically, a key creation function has nothing to do with the routing technique. However, the route in most of RKPD techniques, such as the general process, is set up via a routing mechanism. That is, a dynamic routing techniques needs to be used along with those key sharing process, which will seriously affect the scalability of those RKPD techniques. Moreover, the number of node of the route may improve because the adjacent hops in the route must be logically connected. In fact, the whole amount of computation rate for deciding whether a distributed key exists in key range of two adjacent hops is also very large because the routing function may involve more nodes.

The general steps of Phase 3 are changed, and a route that the adjacent nodes only need to be physically connected can be getting by real routing techniques. To decrease the transmission overload, a start-based method is used to select key range for all nodes upon the input of node's identifier. Although the start-based method has been mentioned, we earlier build a deterministic mechanism, with which the times that each key is choose by nodes approximate the average rate.

2.3.1 The Scheme

Phase 1 (key pre-distribution)

Early the used of nodes, for all node, a main control dynamically select a key range and stores it into the node. RKP mechanism has more parameters. Here use a key pre-distribution technique that relies on probabilistic key distribution between nodes within the sensor network. Their system works by sharing a key range to each participating node in the sensor network early deployment. This key engagement problem is a part of the key maintenance risk, which has been rarely studied in basic network environments. There are three types of basic key agreement techniques: trusted-server mechanism, self-enforcing technique, and key pre-distribution process. The trusted-server mechanism dements on a trusted server for key engagement among nodes. This type of technique is not matched for sensor networks because there is normally no security environment in sensor networks.

Step 1: The main control dynamically creates keys and develops a particular key identifier to all; those keys and the corresponding identifiers connect a key pool.

Step 2: The main control selects a deterministic mechanism to assign the key identifiers provides to each node on the input of the node's identifier.

Step 3: For each node, the main control inputs its identifier into and output distinct rates among and, denoted by At last, the main control create keys whose key identifiers are.

Phase 2 (shared key discovery)

The shared-key discovery part takes position while DSN initialization in the performance infrastructure where each node discovers its nearby node in wireless transmission ranges with which it distribute keys. The easy way for any two nodes to determine if they distribute a key is that each node transmit, it has in mind, the list of identifiers of the keys on their key range. This process does not give an adversary any malicious behavior that he does not earlier have. For example, if an adversary gathers a node he can determine which key of that node is used for which connection by decrypting transmission; and if he does not gather a node, the adversary can mount a congestion analysis malicious in the omission of key identifiers.

The shared-key discovery model describes the range wise anatomy of the sensor array as seen by the routing phase of the DSN. A connection exists among two sensor nodes only if they distribute a key; and if a connection exists among two nodes, all transmission has trusty by link encryption. Notice that it is possible that the same key is distributed by more than a pair of sensor nodes.

Step 1: Each node transmits its identifier and reports the gathering identifiers, denoted by .For each node, node runs the function and assigns the key identifier set of nodes.

Step 2: If there is a general key identifier in such set and its own key range, they are intra based connected. Then node adds a report mentioning the node identifier and the same key identifier to its nearby node list.

Algorithm 2.3.1 Key Pre-distribution

1: for Each element b in GF(p) d, c in GF(p) do, y in GF(p) do

2: x = −(c + by)

3: Assign key (x, y, 1) to node (1, b, c), end for

4: Assign key (−b, 1, 0) to node (1, b, c)

5: end for

6: for Each element c in GF(p) do, x in GF(p) do

7: Assign key (x, −c, 1) to node (0, 1, c), end for

8: Assign key (1, 0, 0) to node (0, 1, c), end for

9: for Each element x in GF(p) do

10: Assign key (x, 1, 0) to node (0, 0, 1), end for

11: Assign key (1, 0, 0) to node (0, 0, 1)

Phase 3 (path key establishment)

The path-key generation model creates a path key to choose couple of sensor nodes in the wireless communication ring that do not have a normal key, but are connected by pair or more connection at the end of the shared-key discovery level. Path keys need not be created by sensor nodes. The design of the DSN ensures that, later the shared-key discovery model is ended a number of keys on a key range are left without generates to any connection. For instance, both analysis and simulations indicate that even without particular provisioning a substantial bit of keys are left unused on key ranges. Provisioning for acceptable ring keys that are left unassigned by the discover of key-ring size (k) can also anticipate both the effects of avoidance and those of incremental gain of new sensor nodes, since both may require the carrying out of the path key generation model later shared-key discovery.

Algorithm 2.3.2 Shared Key Discovery

1: if ai = 0 and bi = 0 and ci = 1 then

2: if aj = 0 and bj = 1 then

3: Identifier of the common key = (1, 0, 0), else

4: Identifier of the common key = (−bj, 1, 0), end if

5: else if ai = 0 and bi = 1 then, if aj = 0 and bj = 1 then

6: Identifier of the common key = (1, 0, 0), else

7: Identifier of the common key = (bj ci − c j ,−ci, 1), end if

8: else {When (ai , bi , ci) = (1, b1, c1) and (aj , bj ,c i) = (1, b2, c2)}

2.3.2 Key Identifier Set Generation

Generate a one-dimensional array of size and initialize the array with “0”s. After the following levels, output the array which is accepted with key identifiers for a node. For each (1)the LFSR shift to build bit stream; (2)once every bits have been established, compute rate ; (3)if or , go to (1); (4)else, ; (5)sort the sequence deploying standard insertion sort model end for.

2.3.3 Security Model

Trusty is a mainly used term encompassing the parameters of security, quality, privacy, non repudiation, and anti-playback. The more the dependency on the information gives by the networks has been improved, the more the risk of trust transmission of information over the networks has improves. The secure communication of different types of information over networks, several cryptographic, steganographic and other models are used which are well known.

3. EXPERIMENTAL RESULT AND DISCUSSION

This research work used ns-2 as the network simulator and participates various simulations to implements the E2S2 performance. All sensor nodes are dynamically scattered with a same distribution. The range of the sink is randomly described. This model evaluates the routing performance under scenarios with various numbers of sensor nodes.

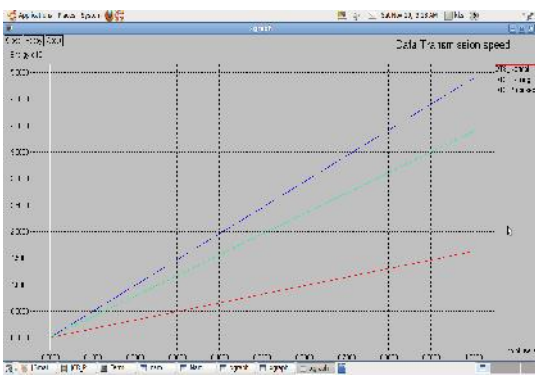
This simulation process conducts the following main performance parameters:

1) Data Transmission speed: the ratio of the data sending amount of speed the sink gets to the overall number of messages from the start node sends.

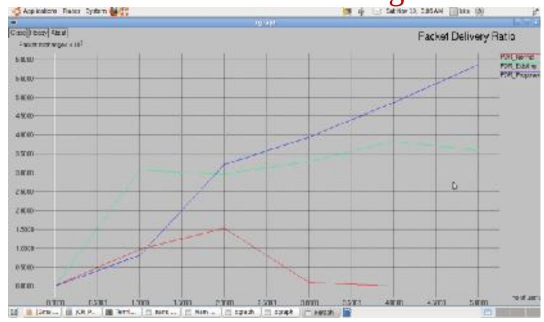
1) Packet deliver Ratio: the ratio of the number of data the sink gets to the total number of messages from the start node sends.

2) Throughput ratio: measures the mean value of the data rate of all live sensor nodes when simulation terminates.

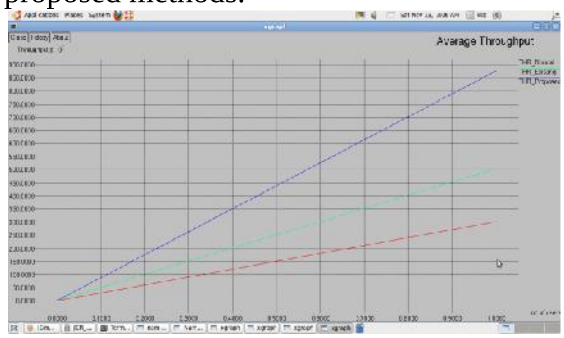
3) End-to-end Delay: means the time delay experienced by the source node while transmitting a report message to the sink.



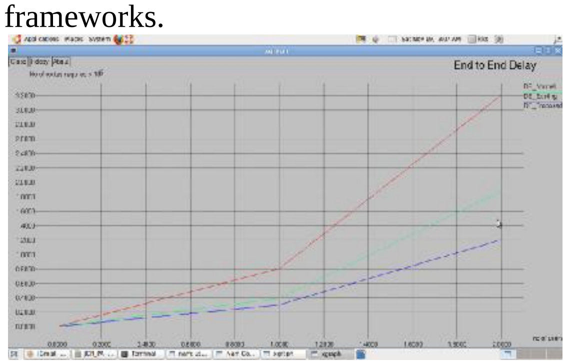
The figure 3.1 Data transmission speed compare the proposed transmission speed ratio increased comparing to existing and proposed methods.



The figure 3.2 Packet Delivery Ratio compare the proposed modification Delivery Ratio increased comparing to existing and proposed methods.



The figure 3.3 Throughput Ratio, compare the proposed modification high ratio comparing to existing and proposed frameworks.



End-to-End Delay compare the proposed modification low delay ratio comparing to existing frameworks.

Parameters comparison Table with previous frameworks:

Parameters	LEACH	BSC	Existing JCR	Proposed E2S2
Life Time	6,445s	7,250s	7,450s	8,150s
Transmission Speed	Light high	Light high	high	Very high
Throughput	250 pkts	295 pkts	300 pkts	340 pkts
End-to-End Delay	0.047s	0.045s	0.044s	0.042s
Packet delivery Ratio (25 sec)	65	70	78	96

Above performance discussion phase we give details of simulation performance and snap shots for used techniques comparison for previous and current techniques results in graphical representation. In general, the nodes along the routing path are likely to exhaust their battery energy rate quickly when request increases. This may cause data reconstruction to determine a new route, thereby improving the delivery data rates. The proposed mechanism gives better delivery latency.

CONCLUSION

In this process the framework of random key pre-distribution to address the bootstrapping problem. First, we propose the random key pre-distribution scheme, which achieves greatly strengthened authentication by small range malicious while reduced improving security in the face of a large scale physical attack on network nodes. We will explain why this trade-off is a desirable one. And then, we use the multiple route secure process, which substantially improves the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising any given communication.

At last, we use the random-pair-wise keys techniques, which assures that, even when some number of nodes have been compromised, the remainder of the network remains fully trusted. Avoidance of a attacker node is most particular in key sharing scheme. Increased energy efficiency Reduced energy consumption.

REFERENCE

[1] J. Stankovic, “Research directions for the internet of things,” Internet of Things Journal, IEEE, vol. 1, no. 1, pp. 3–9, Feb 2014.

[2] Y. Liu, X. Mao, Y. He, K. Liu, W. Gong, and J. Wang, “Citysee: not only a wireless sensor network,” IEEE Netw., vol. 27, no. 5, pp. 42–47, September 2013.

[3] T. H. Luan, L. X. Cai, J. Chen, X. Shen, and F. Bai, “Engineering a distributed infrastructure for large-scale cost-effective content dissemination over urban vehicular networks,” IEEE Trans. Veh. Technol., vol. 63, no. 3, pp. 1419 – 1435, 2014.

[4] R. Du, C. Chen, B. Yang, N. Lu, X. Guan, and X. Shen, “Effective urban traffic monitoring by vehicular sensor networks,” IEEE Trans. Veh. Technol., vol. 64, no. 1, pp. 273 – 286, 2015.

[5] X. Tian, Y. Zhu, K. Chi, J. Liu, and D. Zhang, “Reliable and energyefficient data forwarding in industrial wireless sensor networks,” Systems Journal, IEEE, to appear.

[6] C. Chen, J. Yan, N. Lu, Y. Wang, X. Yang, and X. Guan, “Ubiquitous monitoring for industrial cyber-physical systems over relay assisted wireless sensor networks,” Emerging Topics in Computing, IEEE Transactions on, vol. 3, no. 3, pp. 352–362, 2015.

[7] Y. Yao, Q. Cao, and A. Vasilakos, “Edal: An energy-efficient, delayaware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 23, no. 3, pp. 810–823, 2015.

[8] X.-Y. Liu, Y. Zhu, L. Kong, C. Liu, Y. Gu, A. Vasilakos, and M.-Y. Wu, “Cdc: Compressive data collection for wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 8, pp. 2188–2197, 2015.

[9] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, 2002.

[10] O. Younis and S. Fahmy, “Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,” IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, 2004.

[11] V. Pal, G. Singh, and R. P. Yadav, “Balanced cluster size solution to extend lifetime of wireless sensor networks,” Internet of Things Journal, IEEE, vol. 2, no. 5, pp. 399–401, 2015.

[12] S. Fang, S. Berber, and A. Swain, “An overhead free clustering algorithm for wireless sensor networks,” (GLOBECOM’07), Nov. 2007, pp. 1144–1148.

[13] D. Wei, Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, “An energyefficient clustering solution for wireless sensor networks,” pp. 3973–3983, 2011.

[14] N. Amini, A. Vahdatpour, W. Xu, M. Gerla, and M. Sarrafzadeh, “Cluster size optimization in sensor networks with decentralized clusterbased protocols,” Computer Communications, vol. 35, no. 2, pp. 207– 220, 2012.

[15] C. Chen, S. Zhu, X. Guan, and X. S. Shen, Wireless Sensor Networks: Distributed Consensus Estimation. Springer Brief, 2014.

[16] R. Zhang, J. Pan, J. Liu, and D. Xie, “A hybrid approach using mobile element and hierarchical clustering for data collection in wsns,” in pp. 1566–1571.

[17] D. C. Hoang, P. Yadav, R. Kumar, and S. K. Panda, “Real-time implementation of a harmony search algorithm-based clustering protocol for energy-efficient wireless sensor networks,” 2014.

[18] H. Zhou, B. Liu, T. H. Luan, F. Hou, L. Gui, Y. Li, Q. Yu, and X. Shen, “Chaincluster: Engineering a cooperative content distribution framework for highway vehicular communications,” 2014.

[19] O. Demigha, W.-K. Hidouci, and T. Ahmed, “On energy efficiency incollaborative target tracking in wireless sensor network: A review,” IEEECommun. Surveys Tuts., 2013.

[20] F. Ye, G. Zhong, S. Lu, and L. Zhang, “Gradient broadcast: A robust data delivery protocol for large scale sensor networks,” Wireless Networks, 2005.