Contemporary Engineering Sciences, Vol. 7, 2014, no. 10, 491 - 499
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.4444

Energy Competent Cluster Based Prediction Framework for Wireless Sensor Network

A. C. Jayasudha

School of Computing, SASTRA University
Thanjavur-613401, India

Veeramuthu Venkatesh

School of Computing, SASTRA University
Thanjavur-613401, India

Abstract

In wireless sensor networks, sensors unceasingly scrutinize the target environment and impart data to the base station for further resolution. Since it is a resource constraints environment, network lifetime pursues on the battery backup. Hence in this paper, clustering based localized prediction scheme is proposed by exploiting spatial and temporal correlation to have accurate data aggregation and energy efficient network. Cluster updates the history of all sensor values, where cluster member will be in sleep/awake state and adaptively chooses prediction schemes by comparing with error bound range. Key values are generated at each node to contribute authentication process during communication. Thus data aggregation using this algorithm will reduce energy consumption and there is a significant trade-off between communication and computation cost. NS2.29 simulator is used to evaluate the performance of various parameters of protocols such as AODV, DSR, DSDV with our proposed framework.

Keywords: Wireless sensor network, Clustering, Prediction algorithm, Energy efficient, Network simulator (NS2), Network lifetime

1 INTRODUCTION

Preceding with the renovation of engineering technology, Embedded systems plays a leading role in affording real time application, which sophisticate automated system. Belonging to this field, recently there is a drastic improvement in MEMS and actuators [3], which paves way for exploring wireless sensor networks. In an unstructured network, nodes are capable of sensing and adapt according to changes in the environment. An individual sensor node incorporates the functioning of sensing, processing and communicating the sensed data. Hence, lifetime of the node depends on the battery. Increased battery lifetime enhances reliability of the network. Energy conservation prevails as important issue because of resource constraints in WSN. HEED is a distributed cluster algorithm for adhoc network [7], where nodes make use of residual energy and probabilistically elect itself as cluster head [10]. Data driven processing proposes optimized data collection derived from spatial and temporal correlation [6]. This reduces cluster computation and overhead [1]. Distributed approach proposes prediction system, where the trained predictor values are transmitted to base station [8]. Probabilistic robust approximation of predicted value during data collection, that enhances minimum communication cost and detects the events [2]. Energy efficient prediction algorithm proposes adaptive scheme for enabling and disabling prediction operation in a cluster based data collection [4]. comparison analysis of mobile adhoc routing protocol such as AODV, DSR, DSDV and TORA is made and various metrics including PDR, network lifetime, energy consumption, routing overhead and time delay are figure out [5] [9].

2 DESIGN AND IMPLEMENTATION

i) System model:

There are five modules in this system as shown in figure 1

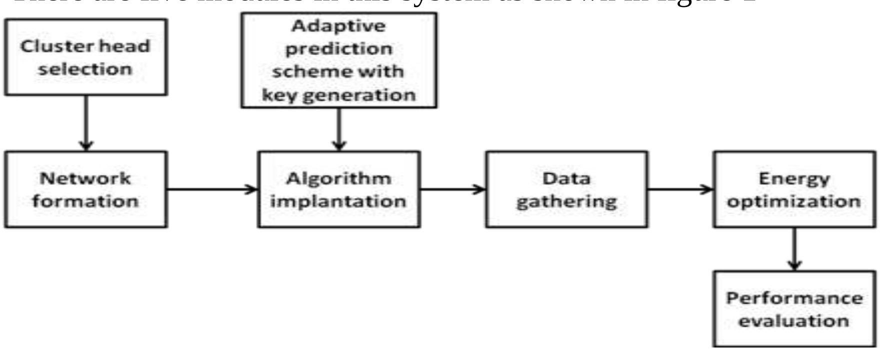

Figure 1: Architecture model for the system

Randomly deployed sensor node are made to form a cluster. Algorithm is implanted in the cluster head and advertise it to all cluster member. Initially, all cluster members remains in sleep mode. After certain time out, nodes which is to be sensed is alone made active. During adaptive data collection, active nodes are verified for their error bound range. If the active node is under the error bound value, it enables the prediction scheme and predicted value is transmitted. If the sensed data does not falls under the error constrain limits, disables the prediction scheme and transmission occurs. cluster head holds the history of updated data. Error bound value is considered to be the least value of energy level that is required for the node to prolong network lifetime and use it for appropriate sensing of data. Besides implementing prediction algorithm, nodes are supplemented with key values generated using RSA algorithm. It pursuits secure cluster based data collection using prediction algorithm. Hence it achieves trade-off between energy consumption and time delay. Performance evaluation of PDR, time delay, throughput, loss rate and energy consumed in various protocol such as AODV, DSR, DSDV is analyzed using NS2 simulators.

ii) System framework and algorithm implemented:

Cluster based localized prediction algorithm exploits spatial and temporal correlation of sensed data. The framework consists of three main function as shown in figure 2;

a) Robust data collection and adaptive update at cluster head by enabling/disabling prediction

b) Generation of key values

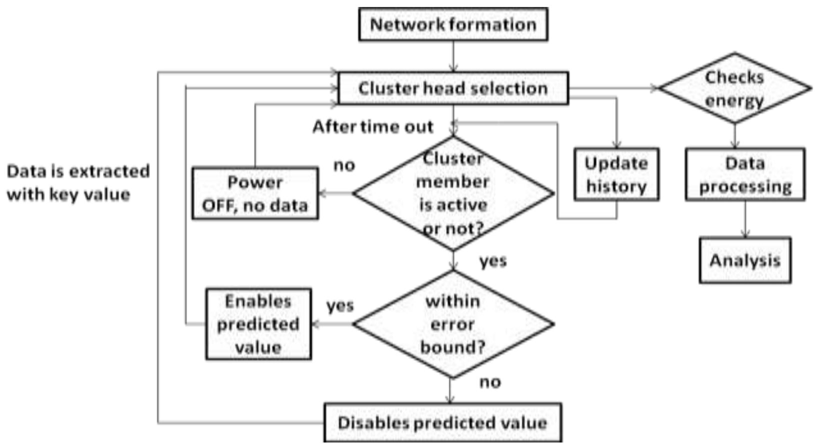

Figure 2: System framework

a) Robust data collection at the cluster head for enabling/disabling prediction:

At every time instance t, each node has an attribute y, generating data value $y_{t.}$ using ∈-loss approximation model, selective data transmission is possible. Data with error bound ∈>0 and $|y-\hat{y}(t)|>\epsilon$, $\hat{y}(t)$ is a value of predictive representative to approximate data value. Parameters calculated using yule walker equation. For a given error bound ∈, confidence level of linear predictor exemplary is described by the following statement;

LEMMA: With the linear predictor Q, estimate $\sum_{j=1}^{p}|\phi_j|\leq 1$ and if it is satisfied, $VAR[E(n)]\leq n^2\sigma^2$ and confidence level is found to be $\hat{y}(t)\pm\phi^{-1}(\beta)n\,\beta$, where ϕ is aggregate distribution function of G(t). In contradiction, with assigned error bound ∈, range of confidence for the predictor will be $\beta_n=2\phi\left(\frac{\epsilon}{SDV\,[E(n)]}\right)-1$, where SDV-standard deviation. Energy efficient scheme is provided by the below statement;

THEOREM: Prediction scheme will become energy efficient if error bound satisfies $\phi(\frac{\epsilon}{n\beta})>\frac{l+1}{2l}$.Hence if correlation coefficient $p_x(b)$ and error tolerant ∈ satisfy

$$\frac{\epsilon}{\sqrt{1-\sum_{b=1}^{Q}\phi_b\rho_y(b)}}>n\sigma_y\phi^{-1}\left(\frac{l+1}{2l}\right) \quad \rightarrow (1)$$

Each sensor node contribute to implement prediction scheme. If the above equation (1) is satisfied, node will not be in error bound range and so transmits data, else predicted value is updated. Below figure shows the description for algorithm using pseudo code. In the figure 3, line 01-06 shows whether scheme enables/disables prediction and line 07-12explains sleep/awake nodes present in the cluster and updates history of data at cluster head

```
Process at the cluster head:
01: if timeout after m*Δ seconds
02:   for each member I in the cluster
03:     if condition (1) holds
04:       sends message to member i to enable prediction
05:     else
06:       sends message to member i to disable prediction
07: else
08:     for each member i in this cluster
09:       if receive a data value from member i
10:         update the history data for member i
11:       else
12:         perform prediction to update the history data
```

Figure 3: Pseudo code for the process taking place at cluster head

Figure 4 shows process taking place at each cluster member. If there is predicted data values from the sensor node then cluster head updates from the history, else sensed data is updated.

```
Process at cluster member:
if prediction is disabled or |x-x_i| > €
      send the data value to the cluster head
      update the history data using data value
else
      perform prediction to update the history data
```

Figure 4: Pseudo code for the process taking place at cluster member

So this algorithm comprising dynamic cluster split and merge is added resulting in reduced communication cost and act as a energy efficient framework.

b) Extended key generation system:

Basically, RSA key generation is a public key cryptosystem which consists of two keys. One is a private key furtive only to the receiver, other public key revealed to all. To increase the authentication, prime number testing algorithm and extended Euclidean algorithm are added. These involves only small computational cost.

3 PERFORMANCE EVALUATION

i) Simulation environment:

The proposed system model is simulated using NS2.29, which is a discrete event simulator. Objects of network components in the data path are compiled using C++. OTCL is used for creating and managing simulation scenario. TclCL act as a linkage between C++/OTCL and to create network topologies. A scripting language called perl is used to interface shell programs for text manipulation. X graph tool will help in plotting and graphing. Their animation is also made visualized in NAM (network animator) by executing trace files from TCL scripts.

ii) Evaluation metrics considered and analysis of simulation result:

The following network criteria are considered;

a) PDR:

PDR is described as total count of packets consists of data arrived at the destination to those originated at the source node. In figure 5, Simulation result implies that proposed system slowly decreases for the given simulation time. our system has comparatively higher PDR percentage whereas DSDV has lowest percentage.

Table 1: Parameters assigned in the simulation

Simulation parameter	Value
Simulation time	50ms
Interface queue	Droptail/priority queue
Channel type	Wireless channel
Number of packets in the queue	50
Topology size	1000mx1000m
Total count of nodes	100
Type of MAC layer	IEEE802.11
Pause time	10ms
Initial energy	50nJ
Range for radio propagation	250m
Transmit power	1.0W
Receive power	1.0W
Idle power	1.0W
Traffic pattern	CBR
CBR packet rate	128 packets
Connectivity count	30
Routing protocols	AODV, DSR, DSDV

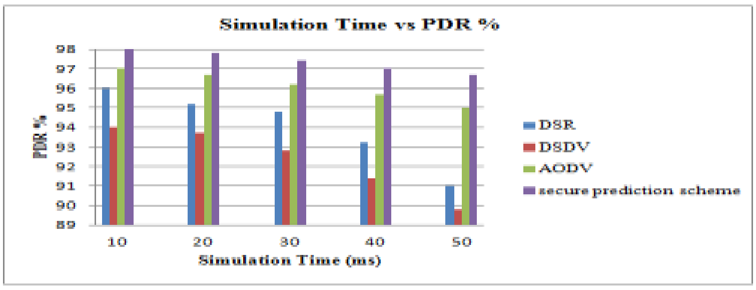

Figure 5: Analysis of Simulation time vs PDR for AODV, DSR, DSDV and secure prediction scheme

b) Throughput:

Total count of packets received by the destination node in accordance with ms is denoted as throughput rate. In figure 6, analysis shows that for every ms, total number of packets arrived at sink node measured in Kbps is comparatively higher for secure prediction scheme and DSDV has the lowest rate.

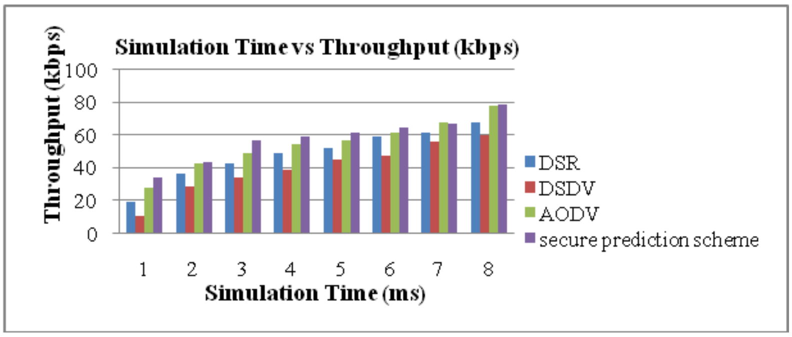

Figure 6: Analysis of Simulation time vs Throughput for AODV, DSR, DSDV and secure prediction scheme

c) End-End time delay:

It is referred as the ratio of time gap among first and next packet transmitted to the total number of packets delivered. Figure 7 shows that our system remains constant throughout the simulation time and has lowest delay time, whereas DSDV has higher delay time.

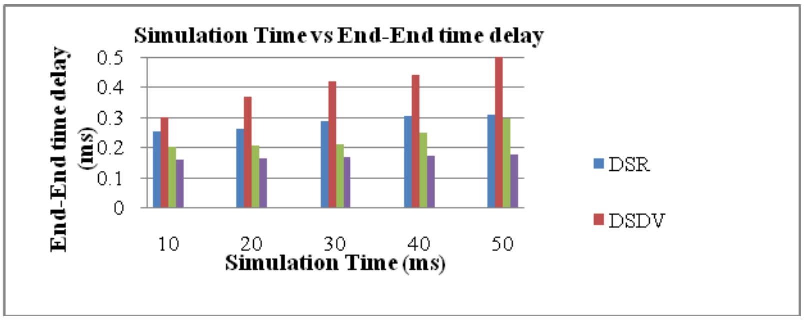

Figure 7: Analysis of Simulation time vs End-End time delay for AODV, DSR, DSDV and secure prediction scheme

d) Loss rate:

It denotes the percent of number of packets dropped at the destination. Figure 8 shows that our proposed work drastically decreases throughout the simulation time and has lower loss rate, whereas DSDV holds higher loss rate.

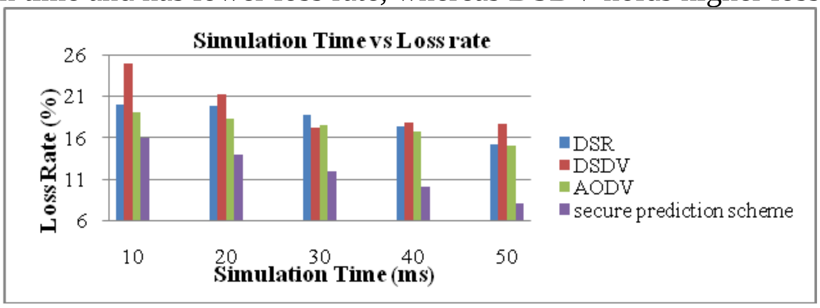

Figure 8: Analysis of Simulation time vs loss rate for AODV, DSR, DSDV and secure prediction scheme

e) Remaining energy:

It is the amount energy residing in the node after event is completed, calculated at every pause time. In figure 9, graph shows that for every pause time total remaining energy exponential increases for our proposed work and has larger remaining energy, DSDV has small amount of residual energy.

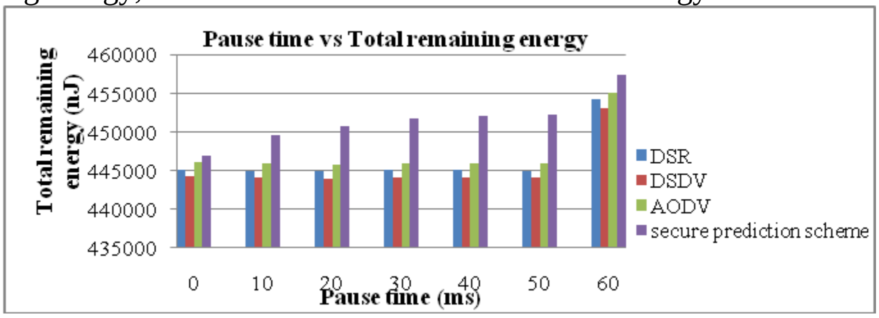

Figure 9: Analysis of Pause time vs Total remaining energy for AODV, DSR, DSDV and secure prediction scheme

CONCLUSION AND FUTURE WORK

From the comparative simulation of energy consumed by secure prediction scheme, AODV, DSR, and DSDV, our proposed secure prediction framework is found to be energy efficient. Also the performance evaluation and comparison of various parameters for AODV, DSR, DSDV and our proposed scheme implies that, secure prediction algorithm has low loss rate, end to end delay, average utilization and high PDR, throughput, total remaining energy against simulation time. Thus our proposed energy efficient framework has good performance and among the comparison protocol DSDV has poor performance. In future we can implement mobile sensor nodes in this algorithm.

REFERENCES

[1] A. Silberstein, R. Braynard, G. Filpus, G. Puggioni, A. Gelfand, K. Munagala, and J. Yang, Data-Driven Processing in Sensor Networks, Innovative Data Systems Research (CIDR), Proceedings Conference, 2007.

[2] C. David , D. Amol Deshpande, M. H. Joseph, H. Wei, Approximate Data Collection in Sensor Networks using Probabilistic Models, Data Engineering, 22nd Proceedings International Conference, 2006.

[3] F. L. LEWIS, Wireless Sensor Networks, Smart Environments: Technologies, Protocols, and Applications, The University of Texas, Arlington, 2004.
[4] J. Hongbo, J. Shudong Jin, and W. Chonggang, Prediction or Not? An Energy-Efficient Framework for Clustering-Based Data Collection in Wireless Sensor Networks, IEEE Transactions On Parallel And Distributed Systems 22(6), June 2011, 1064-1071.
[5] K. Mina, J. Shahram, G. Sajjad Jahanbakhsh, Performance Comparison of AODV, DSDV, DSR and TORA Routing Protocols in MANETs, Journal of Applied and Basic Sciences (2012), 1429-1436.
[6] L. Chong, W. Kui, P. Jian, An Energy-Efficient Data Collection Framework for Wireless Sensor Networks by Exploiting Spatiotemporal Correlation, IEEE Transactions On Parallel And Distributed Systems 18(7) (2007), 1010-1023.
[7] M. Faheem, B. N. Asri, S. Ali, M. A. Shahid and L. Sakar, Energy based Efficiency Evaluation of Cluster-Based Routing Protocols for Wireless Sensor Networks (WSNs), International Journal of Software Engineering and Its Applications 7 (6) (2013), 249-264.
[8] S.M. McConnell and D.B. Skillicorn, A Distributed Approach for Prediction in Sensor Networks, Data Mining Workshop Sensor Networks (SIAM), Proceedings International Conference, 2005.
[9] W. Hongjun, S. Zhiwen, N. Xiaoyu, D. Qun, Key Generation Research of RSA Public Cryptosystem and Matlab Implement, Sensor Network Security Technology and Privacy Communication System, International Conference, 2013.
[10] Y. Ossama, and F. Sonia, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks, IEEE Transactions On Mobile Computing, 2004.

Received: April 3, 2014