Analysis on Disconnected Nodes in Wireless Sensor Networks

Mukesh Kr. Gupta
Department of Computer Science Engineering
Bengal institute of technology & management (BITM)
Santiniketan, , Doranda, Birbhumn WB, Pin: 731236

Jayashri Deb Sinha
Department of Computer Science Engineering
Bengal institute of technology & management (BITM)
Santiniketan, , Doranda, Birbhumn WB, Pin: 731236

***Abstract*— In a wireless sensor network existence of disconnected node is a common issue. Sensor devices, deployed under adverse environmental conditions, often lose their normal communication capability due to shrinkage of the communication radius. Numerous research works have corroborated this with hardware test results. In this paper we consider both temporary and persistence disconnections of sensor devices from the network. We present a probabilistic model that describes the probability of disconnection in terms of node density and communication radius. We also present simulation experiments that clearly differ networks with disconnected nodes from normally connected nodes. Our simulation experiments also report a 50% degradation the throughput and 28% extra energy depreciation with the occurrence of disconnected nodes in the network. The analysis and simulation experiments led us to enlist some open research issues in the concluding section.**

Keywords—Wireless sensor network, disconnection, network simulator-3,

I. INTRODUCTION

Wireless sensor networks (WSN) serve numerous applications needs for our day today life [1]. To serve different applications, such as field monitoring, Environmental data collection, Forest fire detection etc. sensor devices are often deployed under environmental adverseness. Harsh environmental condition reduces the normal communication range of a sensor device [2]. Due to this reduction the sensor node becomes disconnected from the network. However, this disconnection has no fixed time interval and other interesting properties as well.

Several research works have proven the shrinkage of communication radius under poor environmental conditions with hardware test results. For example, authors in [3] has shown a 60% shrinkage in communication boundary with increasing temperature from 25°C to 65°C. Their experiments were carried out on Telos Class motes reported 8 dB RSSI loss at 65 °C. Not only conventional Communication protocols like IEEE 802.11 or IEEE 802.15.4 zigbee suffer environmental adverseness, latest communication long distance Communication protocols like LoRAWAN, Sigfox etc. also exhibit disconnection and shrinkage of communication range under adverse environmental condition [4]. For example, Authors in created a setup with 915 MHz LoRa using Raspberry Pi and Dragino LoRa shield hardware platform [5]. Their outcome presented that the effect of humidity and temperature on the sensor device is far more detrimental than rainfall and snow. Additionally, they established a statistical co-relation between the humidity and temperature of inside and outside of an experimental device. In another similar approach authors tested the propagation of 433 MHz LoRAWAN under rubber tree forest area. The results of this study also reported a significant degradation in RSSI with increasing forest density and other environmental issues[6].

Since shrinkage of the communication range is a common phenomenon for both conventional and modern communication protocols. Disconnections of the devices from the network also becomes inevitable issue. Moreover, primitive network management techniques like rate adaption and others do not provide solution to these kinds of problems [7]. With the intention to study the properties and effects of such disconnection, we organize the remaining parts of the paper as follows. SEC -III discusses about some common properties of disconnected nodes. Here, we present a probabilistic model that analyzes the probability of disconnection. SEC-IV presents simulation results which explains the effects of disconnected nodes in the network. In accordance, we enlist some open research issues in the concluding SEC-V.

II. PROPERTIES OF DISCONNECTION

As a sensor device experiences external environmental hazards its communication radius shrinks and it becomes disconnected from the network. However, this disconnection has several interesting properties to discuss.

A. Probability of Disconnection

The disconnection of a node from the network depends on the shrinkage of the communication radius. We can show that the probability of disconnection depends on the average density of deployment [8].

Theorem 1: The probability of disconnection of a node from the network depends on the deployment density.

Proof: Let us consider a network on K nodes deployed in A area with node density (K/A). Now if the communication radius of a node shrinks to R unit distance, there will exist λ nodes in the πR^2 region. Now λ can be formulated as shown in equation no 1. With the help of [9]

$$\lambda = \frac{K}{A}\pi R^2$$

Therefore, the probability P{X=0}, that there will be no nodes in the πR^2 region will be

$$P\{X=0\} = \frac{e^{-\lambda}\lambda^{x}}{x!}$$

Putting the values of λ and x we get,

$$P\{X=0\} = \frac{e^{-\frac{K}{A}\pi R^2}\left(\frac{K}{A}\pi R^2\right)^0}{0!}$$

$$Hence,\ \ P\{X=0\} = e^{-\frac{K}{A}\pi R^2} \quad (1)$$

Equation: 1, establishes the correlation between Node Density and Shrinkage of communication radius. If we consider that at a particular time instance communication radius (R) remains constant P{X=0} becomes directly proportional to Node density (K/A). This proves the statement of the theorem.

B. Duration of Disconnction

- As the disconnection depends on environmental adverseness, The time duration of such this connection is purely random in nature [10].
  If a node remains disconnected and connected for T_D and T_A unit time durations. and the outcome of the node is traced for Δt time units, Then the link throughout (T_h) becomes

$$T_h = \frac{(P_t\, T_A)\ \Omega}{\Delta_t} = \frac{(P_t\, T_A)\ \Omega}{T_A + T_D} \quad (2)$$

  Here P_t is the average packet disbursement rate (in unit time) with packet size Ω.
  Corollary: Link throughput is directly proportional to Connected time interval.
  Proof: We use Equation 2 to prove our notion

$$T_h = \frac{(P_t\, T_A)\ \Omega}{T_A + T_D}$$

  Where,

$$\Delta_t = T_A + T_D$$ is the observation interval that can be considered as constant.

  Similarly,

P_t and Ω can also be considered to be constants that remains unchanged during simulations as well.
Therefore,

$$T_h = T_A \times Constants$$

Or, $$\boxed{T_h \propto T_A}$$

Which institutively, expresses that Link throughput is directly proportional to the connected time interval.

- Additionally, sensor devices can automatically re - establish their connectivity with the appearance of favorable weather condition. Therefore, the ratio between T_D and T_A is stochastic nature. In the simulation, we randomize this co relation and observe the variation of throughput in figure-1.

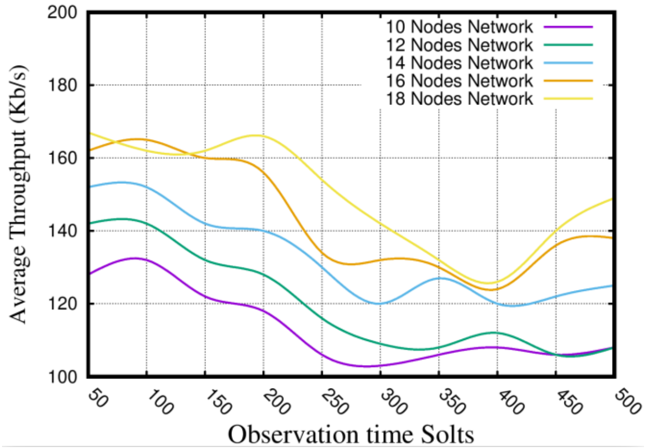

Figure 1 : Changes in throughput with time

III. PERFORMANCE ANALYSIS

To analyze the effects of disconnected node and disconnection interval we simulated a several network scenarios with the following simulation parameters.

A. Simulation Parameters

We use network simulator-3 (ns-3) to simulate disconnected network conditions [11]. Although ns-3 is a discrete event simulator, yet continuous submission of task keeps the clock active throughout the simulation period. Thus, we track the time and schedule the activity of different nodes on different times.

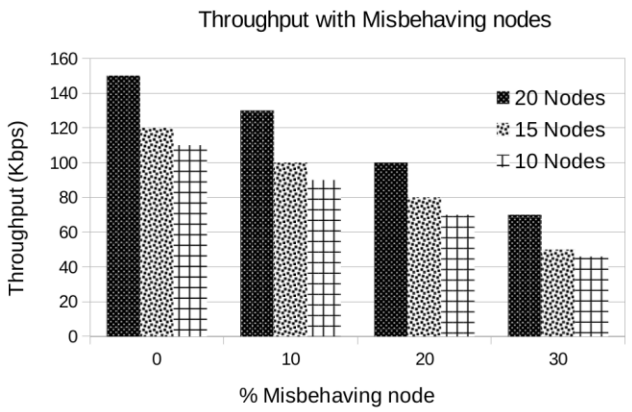

Figure 2: Throughput with changing number of disconnected nodes.

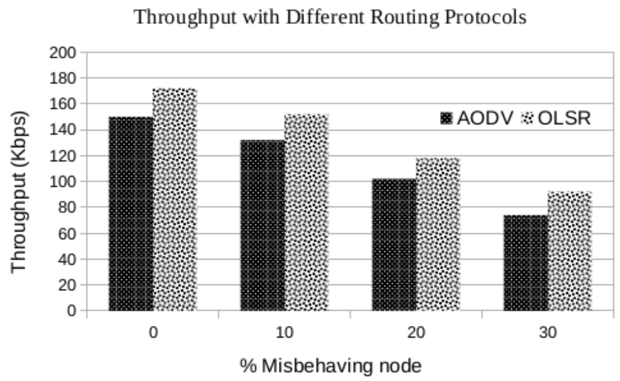

Figure 3 : Change in throughput with different routing protocols.

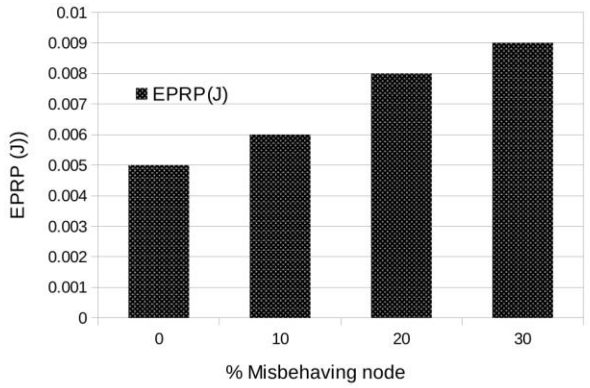

Figure 4: Energy per received packet (in Joule)

B. Results

In our first experiment we deploy 10 -18 nodes over 300 m x 300 m terrain. We discontinue the normal transmission ability of the node by impairing default Send() methods. We schedule this disconnection (T_D) for a pseudo time interval for selected nodes. Figure 1 shows the variation in the collected throughput in different time intervals. We observe a sharp decrease in throughput in the network with 18 nodes topology during 200s to 400s observation intreval, Occurrence of multiple disconnected nodes in a same reason can be considered as the main reason behind this [12].

In our second experiment we gradually increase the percentage of disconnected nodes in the network. The results in figure 2 shows that with the increase of disconnected nodes from 0% to 30% a degradation in throughput observed is almost 50 % in 20 node topologies.

In accordance we deploy 20 nodes in 400 m x 400 m area uniform randomly. We observe the throughput with AODV and OLSR routing protocols with default set ups presented in ns-3. The resulting figure exhibits that in all test cases OLSR outperformed AODV routing protocol. For example, we observe a 28% extra network throughput with OLSR (compared to AODV) having 30% misbehaving nodes in the network. The results of this experiment also corroborates the findings of [13][14].S

In our final simulation we deploy 20 modes in 400 m x 400 m deployment area with initial energy budget 100J (total). We track energy per received packed and plot Figure 4. We observe a significant decrement (30 % approx.) in energy utilization with 30% disconnected node.

IV. CONCLUSION

With the analysis and simulation results we have corroborated the existence of disconnected nodes. We feel the discussion is essential since it is an inevitable issue, mostly in networks with outdoor deployment. Several techniques have been proposed to alleviate the effects of this problem. However, there are several issues which can be considered future work.

- Co-existence of disconnected and connected node creates disconnected topological segments which needs to be connected with minimum latency paths. Therefore, an improved routing protocol which accounts disconnected nodes separately can be an interesting future work.
- Almost all recovery mechanisms focus on distributed recovery or self-detection principle. However, they overlook security concerns like node hijack or malicious node insertion etc [15] [16]. Therefore, a recovery mechanism with security concerns will improve both performance and robustness of the network.

REFERENCES

[1] Xu, Ning. "A survey of sensor network applications." IEEE communications magazine 40.8 (2002): 102-114.
[2] Misra, Sudip, et al. "Existence of dumb nodes in stationary wireless sensor networks." Journal of Systems and Software 91 (2014): 135-146.
[3] Bannister, Kenneth, Gianni Giorgetti, and S. K. Gupta. "Wireless sensor networking for hot applications: Effects of temperature on signal strength, data collection and localization." Proceedings of the 5th Workshop on Embedded Networked Sensors (HotEmNets' 08). 2008.
[4] Das, Subhransu, Pushpendu Kar, and Subhabrata Barman. "Analysis of IEEE 802.11 WLAN frame aggregation under different network conditions." 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 2017.
[5] Riegsecker, Austin. Measuring Environmental Effects on Lora Radios in Cold Weather Using 915 MHz. Diss. Purdue University, 2018..
[6] Ahmad, Khairol Amali, et al. "Impact of foliage on LoRa 433MHz propagation in tropical environment." AIP Conference Proceedings. Vol. 1930. No. 1. AIP Publishing LLC, 2018.
[7] Das, Subhransu, Subhabrata Barman, and Suman Bhunia. "Performance analysis of ieee 802.11 rate adaptation algorithms categorized under rate controlling parameters." Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies. 2014.
[8] Das, Subhransu, Pushpendu Kar, and Dipak Kumar Jana. "SDH: Self detection and healing mechanism for dumb nodes in wireless sensor network." 2016 IEEE Region 10 Conference (TENCON). IEEE, 2016.
[9] Ross, Sheldon M. Introduction to probability models. Academic press, 2014.
[10] Das, Subhransu, Jayashri Deb Sinha, and Subhabrata Barman. "Effects of Persistent Misbehaving Nodes in Wireless Sensor Networks." Proceedings of the International Conference on Computing and Communication Systems. Springer, Singapore, 2018.
[11] Henderson, Thomas R., et al. "Network simulations with the ns-3 simulator." SIGCOMM demonstration 14.14 (2008): 527.
[12] Das, Subhransu, et al. "Novel Multiparameter Detection and Recovery Technique for Diverse Network Systems." IEEE Systems Journal (2021).
[13] Kar, Pushpendu, Subhabrata Barman, and Subhransu Das. "ISCP: Inter State Changing Problem in Wireless Sensor Network with Dumb-Behaving Nodes." Proceedings of the International Conference on Computing and Communication Systems. Springer, Singapore, 2018.
[14] Kar, Pushpendu, Subhransu Das, and Arun Kumar. "PreCoRe: Predictive connectivity re-establishment in wireless sensor network in

the presence of dumb nodes." TENCON 2017-2017 IEEE Region 10 Conference. IEEE, 2017.

[15] Sudiharto, Dodi Wisaksono, Anton Herutomo, and Yunita N. Rohmah. "The Comparison of Forwarding Strategies between Best Route, Multicast, and Access on Named Data Networking (NDN). Case Study: A Node Compromised by the Prefix Hijack." J. Commun. 12.7 (2017): 426-432.

[16] Rana, Khurram Gulzar, et al. "Detection of malicious node in wireless Ad Hoc network by using acknowledgement based approach." Proceedings of the 2017 the 7th International Conference on Communication and Network Security. 2017.