On the Robustness of Standard Cryptographic Mechanisms in High Mobility RFID Systems

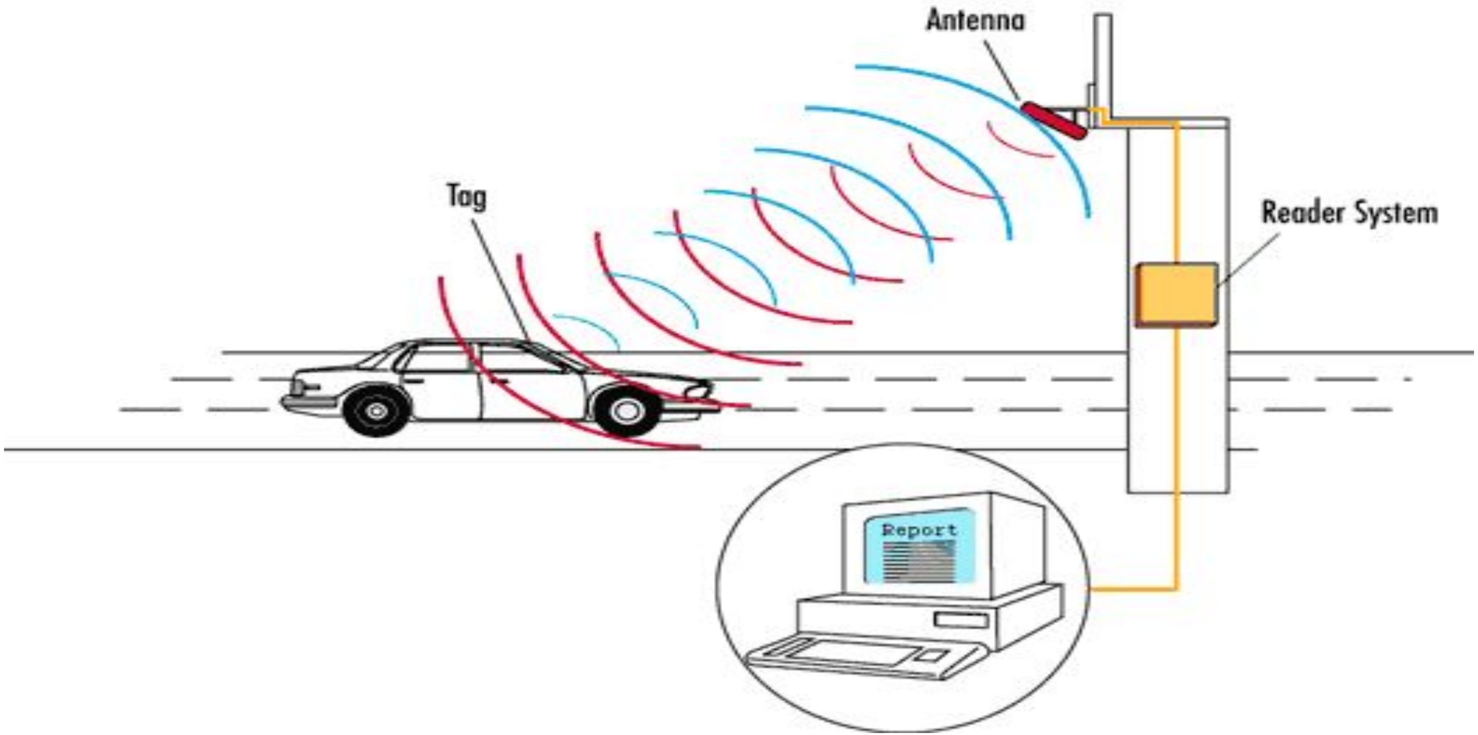
Facilitator :
Prof. Harshan Jagadeesh

Submitted by :
Saurabh 2016EE10825
Shivam 2016EE10160

RFID communication

- ❖ Wireless communication between two entities,namely a reader and a tag.
- ❖ Readers are generally active devices
- ❖ Tags can be active or passive
- ❖ Have a variety of applications. For eg, In IITD library, metro-card authentication, IOTs and much more.
- ❖ Railway uses RFID communication for localization of train.

Schematic of a RFID communication

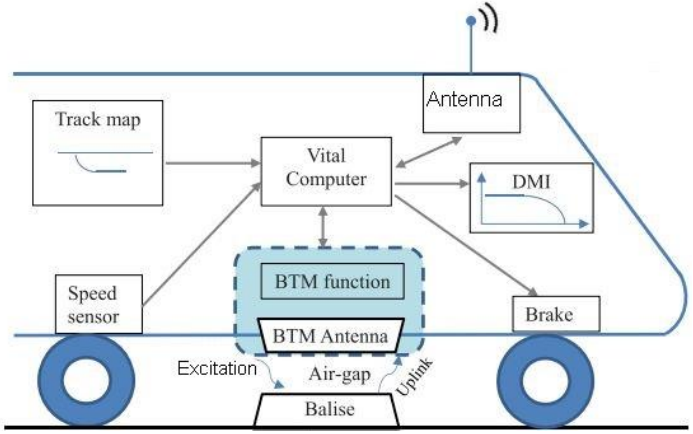


How it works?

- Reader sends activation signal with certain frequency and power.
- The tag gets “activated” from the signal received and responds with the information.
- For instance, the tag ID, or address, or any other important information.
- This communication is not “secure” as no authentication of identity involved.

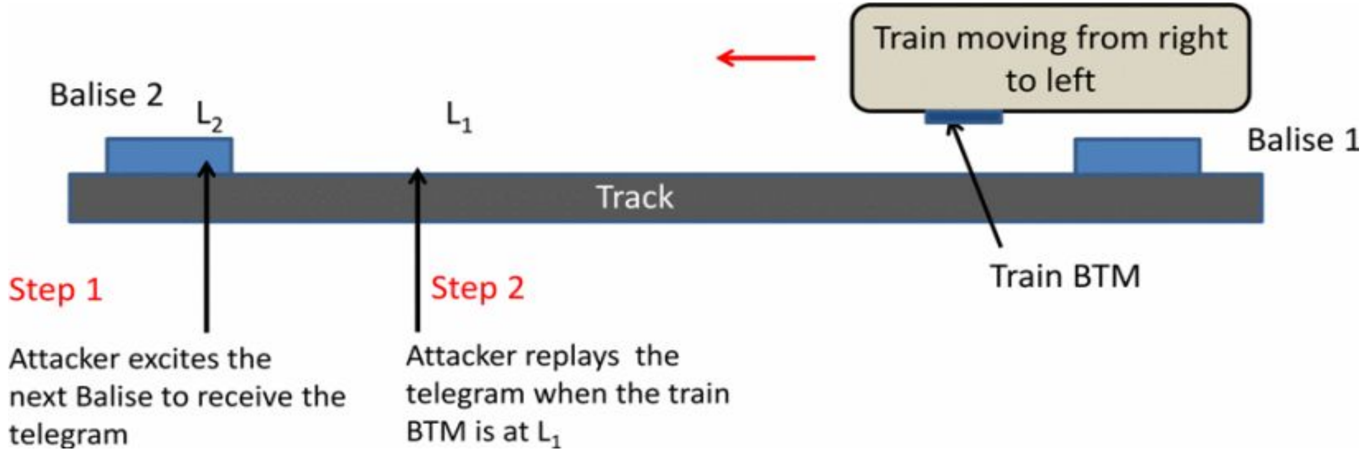
Is security necessary here?

- RFID communication is also used in localization of vehicles like trains. For instance, Delhi metro uses it.
- Also known as BTM(balise-transmission module).



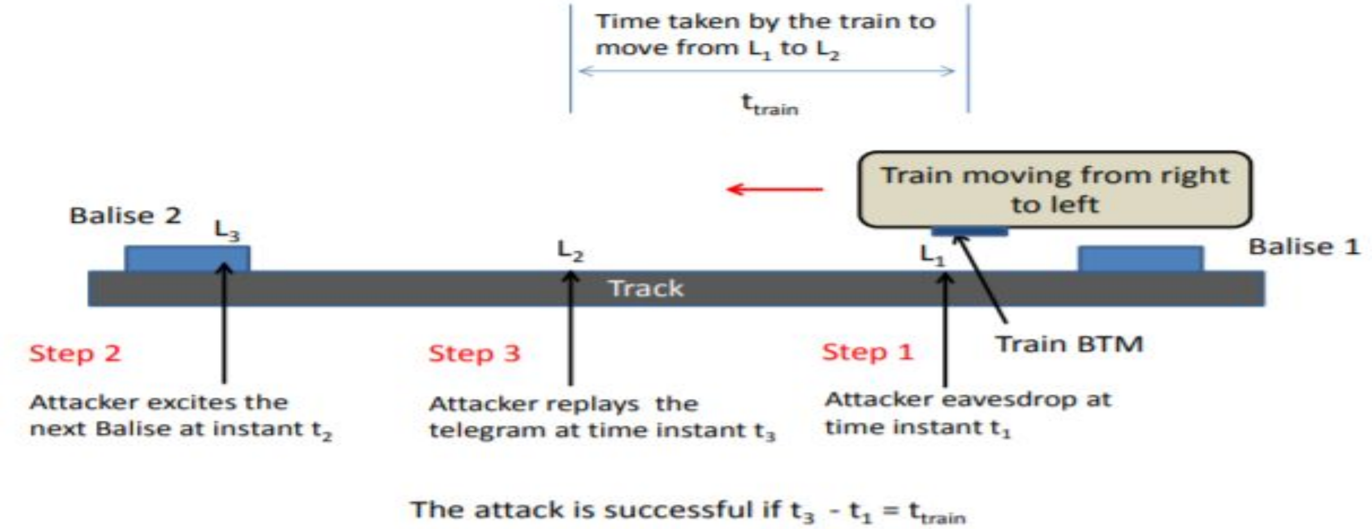
Is security necessary here?

- Various replay attacks exist, through which an adversary can spoof the train location, and this is a serious issue.



Is security necessary here?

- A Sophisticated replay attack which works even when uplink package is MAC secured.



Proposed Mechanism

- Involves three steps with two layers of authentication.
- Train transmits encrypted authentication message.
- This message will be called downlink message.
- Balise decrypts it with a shared key and obtains train ID and a nonce value.
- Balise transmits encrypted MAC and send it back to train.
- This message will be called uplink message.
- Train authenticate the received MAC and localization is completed.

Ballise side authentication mechanism

- Used algorithm for uplink package generation.

procedure BALISE-SIDE ALGORITHM($DL^{(1)}, DL^{(2)}, c$)
    Compute $r \leftarrow D_{k_i}(DL^{(1)})$;
    IF $(r == c + 1) \,||\, (r == c)$
        $k_{BT} \leftarrow MAC_{k_i}(DL^{(2)})$
        Transmit k_{BT} in the uplink telegram
        $c = r$
    ELSE
        Discard the received telegram
    END
end procedure

Train side authentication

- Train also authenticated ballise by using the MAC received.

procedure TRAIN-SIDE RECEIVER(k_{BT}, k_i)

$c \leftarrow MAC_{k_i}(k_{TB})$

IF $c == k_{BT}$

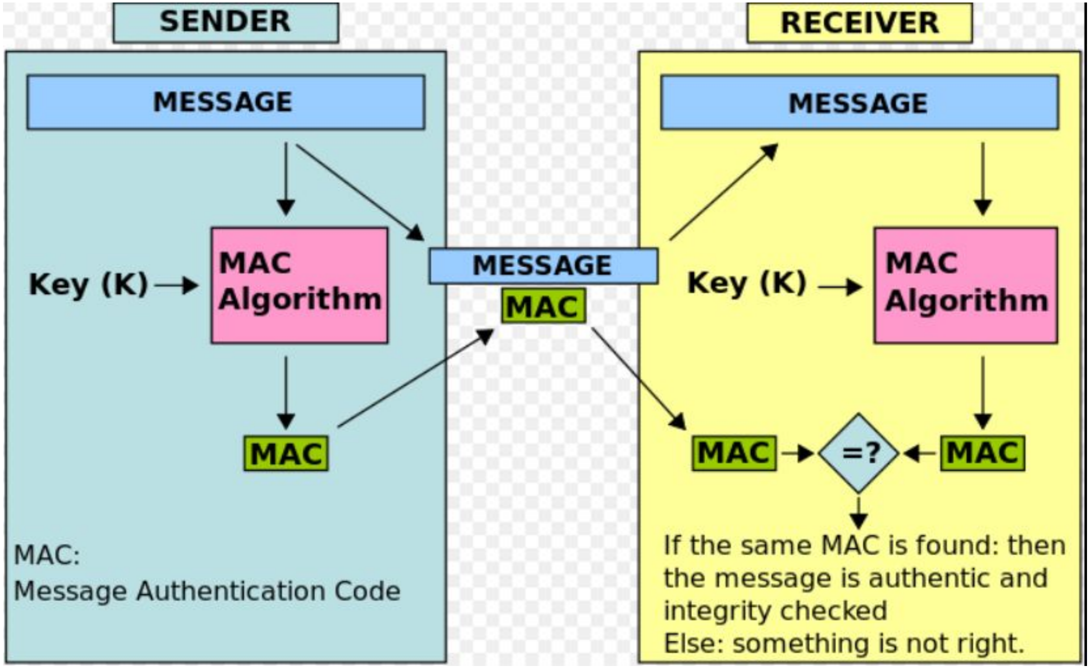
BALISE DETECT $\leftarrow 1$;

Retrieve the encrypted message for the next balise

END

end procedure

Message Authentication Mechanism



Implementation of the Proposed Mechanism

- Literature Survey / Implementation of Cryptographic Algorithms - AES, DES, 3DES, Clefia, Present-80, Salsa, RC-4.
- Clefia, Present-80, AES concluded to be the good for given constraints
- Implementation results inferred that AES performs best.
- Counter Mode(CTR) used for encryption.

	Key size	Block size	Cycles per block	Throughput at 100KHz (Kbps)	Logic process	Area GE	Area rel.
Block ciphers							
PRESENT-80	80	64	32	200	0.18μm	1570	1
AES-128 [16]	128	128	1032	12.4	0.35μm	3400	2.17
HIGHT [22]	128	64	34	188.2	0.25μm	3048	1.65
mCrypton [30]	96	64	13	492.3	0.13μm	2681	1.71
Camellia [1]	128	128	20	640	0.35μm	11350	7.23
DES [37]	56	64	144	44.4	0.18μm	2309	1.47
DESXL [37]	184	64	144	44.4	0.18μm	2168	1.38
Stream ciphers							
Trivium [18]	80	1	1	100	0.13μm	2599	1.66
Grain [18]	80	1	1	100	0.13μm	1294	0.82

Table : Comparison of Lightweight Cipher Implementation ; Source [1]

Algorithm	Average Time taken for encryption
AES - CTR (key size - 128 bits)	5683 ns
AES - CTR (key size - 192 bits)	5824 ms
AES - CTR (key size - 256 bits)	6209 ms
Clefia - CTR(key size - 128 bits)	6969 ns

Table : Performance Comparison of AES and Clefia ; Simulated on N3700

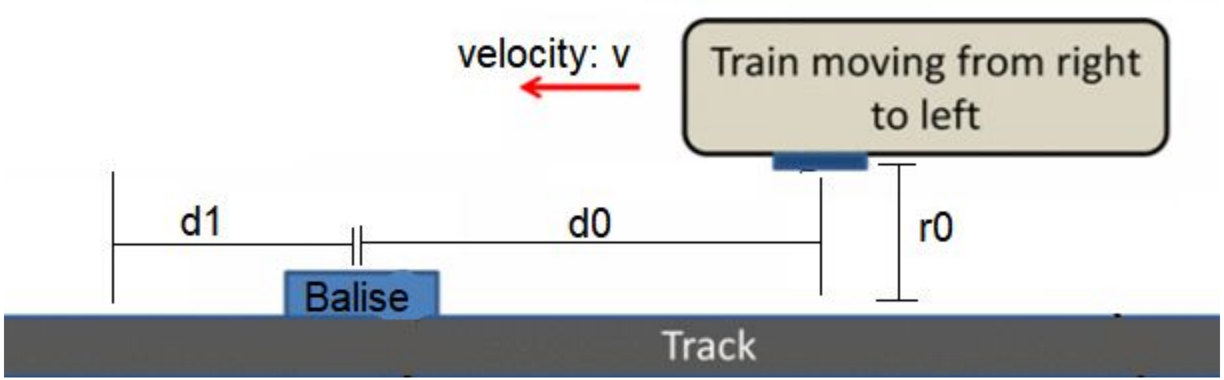
Implementation of the Proposed Mechanism

- Stream Cipher Salsa-20 used for nonce generation
- CRC-8 (0xA6) used for error detection during transmission of message in uplink as well as in downlink.
- White Noise Simulation for(variance - 0.045 to 0.180)

Max length at HD / Polynomial	CRC Size (bits) 3	4	5	6	7	8	9	10	11	12	13	14	15	16
HD=2	2048+ 0x5	2048+ 0x9	2048+ 0x12	2048+ 0x21	2048+ 0x48	2048+ 0xA6	2048+ 0x167	2048+ 0x327	2048+ 0x64D	–	–	–	–	–
HD=3		11 0x9	26 0x12	57 0x21	120 0x48	247 0xA6	502 0x167	1013 0x327	2036 0x64D	2048 0xB75	–	–	–	–
HD=4			10 0x15	25 0x2C	56 0x5B	119 0x97	246 0x14B	501 0x319	1012 0x583	2035 0xC07	2048 0x102A	2048 0x21E8	2048 0x4976	2048 0xBAAD
HD=5						9 0x9C	13 0x185	21 0x2B9	26 0x5D7	53 0x8F8	none	113 0x212D	136 0x6A8D	241 0xAC9A

Table : Best Polynomial at a given CRC size; Source [5]

Simulations & Results



Simulation Model for Computation of Results

Using basic

$$E = \frac{\lambda^2 P_t}{(4\pi)^2 r_0 v}\left[\tan^{-1}\left(\frac{d_1}{r_0}\right) + \tan^{-1}\left(\frac{d_0}{r_0}\right)\right]$$

Parameters Definition

- d1 :The coordinate of the point upto which we are measuring energy accumulated in balise.
- d0 : The largest distance from which the balise could be activated by sending RF signal by train
- r0 : The vertical distance between train and balise. (assumed to be 0.3m)
- Pt: Power transmitted from the train antenna
- Pr : Power received by the balise antenna

Energy accumulated in the Balise

$$E = \int_0^t \frac{D_r D_t \lambda^2}{(4\pi s)^2} P_t \, dt$$

For Isotropic antenna $D_r = D_t = 1$

$$E = \int_0^t \frac{\lambda^2}{(4\pi s)^2} P_t \, dt$$

Substituting, $s^2 = [(d_0 - vt)^2 + r_0^2]$

$$E = \int_0^t \frac{\lambda^2}{(4\pi)^2 * [(d_0 - vt)^2 + r_0^2]} P_t \, dt$$

$$\boxed{E = \frac{\lambda^2 P_t}{(4\pi)^2 r_0 v}\left[\tan^{-1}\left(\frac{d_1}{r_0}\right) + \tan^{-1}\left(\frac{d_0}{r_0}\right)\right]}$$

And, rearranging,

$$\boxed{d_1 = r_o \tan\left(16\pi^2 E \frac{r_0 v}{\lambda^2 P_t} - \tan^{-1}\left(\frac{d_0}{r_0}\right)\right)}$$

Observations and Results

Result 1.

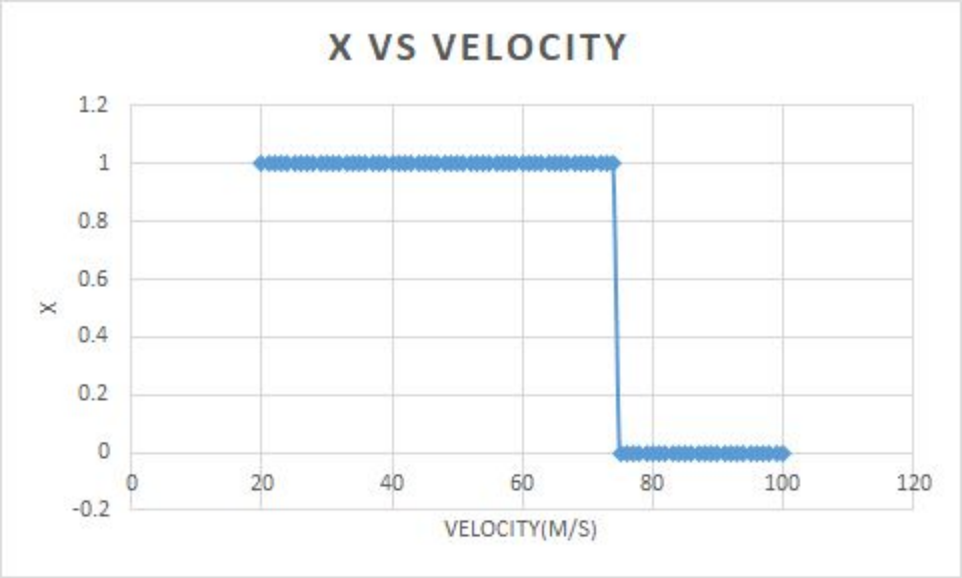
Define a random variable X, representing the likelihood of correct authentication.

$$X = \begin{cases} 1, t_{processing\ time} < t_{face-face\ time} \\ 0, otherwise \end{cases}$$

t_processing time is the total time required for the processing of message in balise
t_face-face time is the total time for which the train is in the interrogation zone of balise

X vs Velocity Graph

Assumptions: Noise Variance is constant (0.045), transmitted power is constant, computational energy is constant.



Authentication Efficiency vs SNR

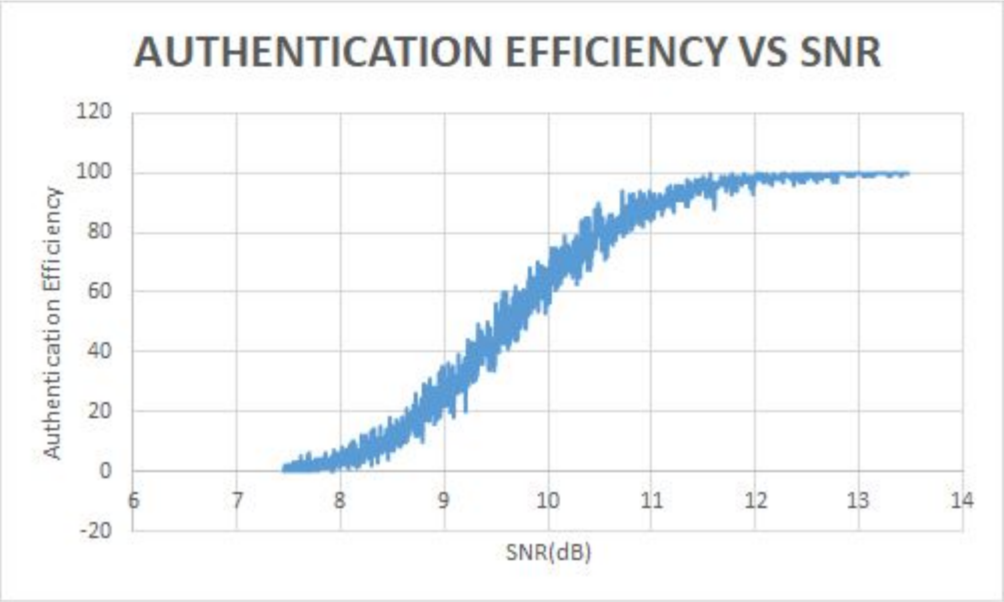


Fig : Velocity of train, v = 60m/s, Power transmitted = 0.5 W

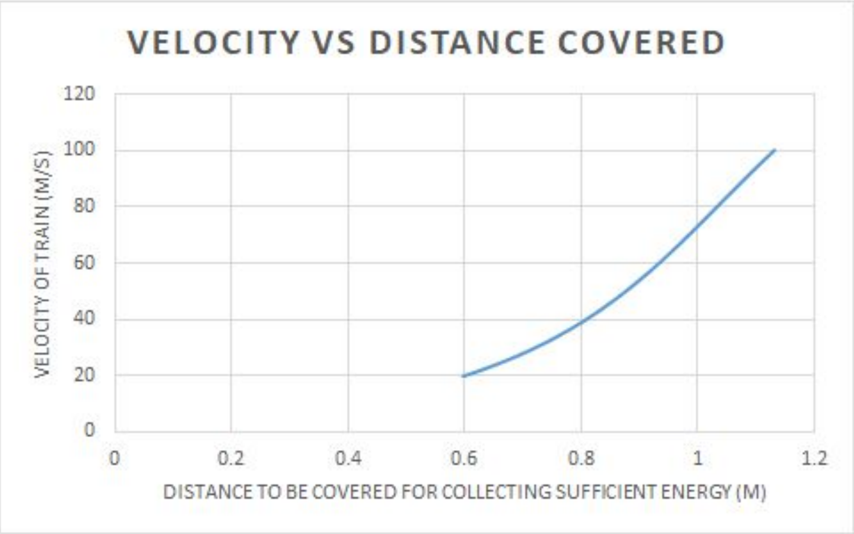
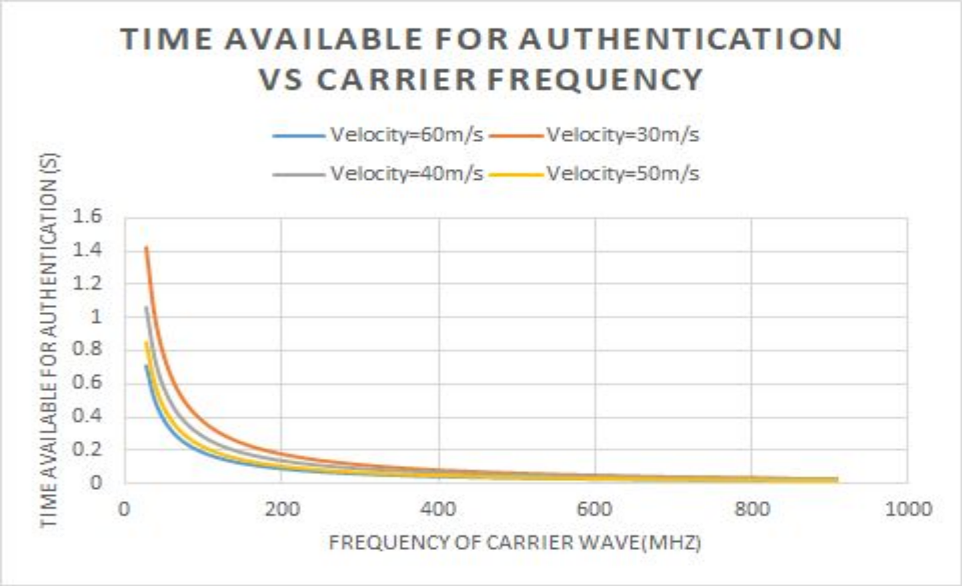


Fig. *Plotted for constant Pt = 1W; d0 = 1.03 m , f = 915 MHz, Noise variance (σ^2)= 0.045*

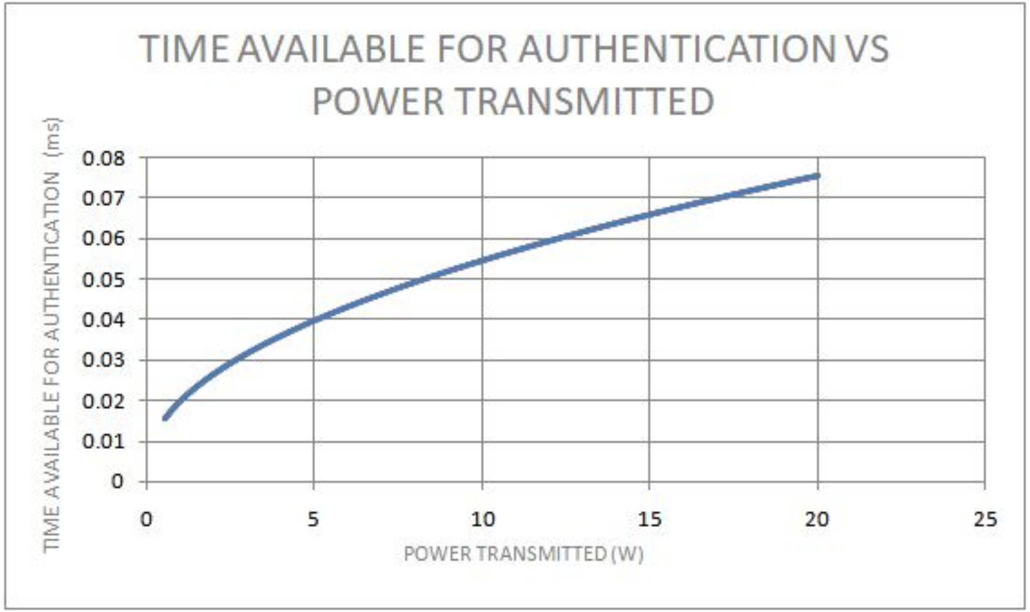
,Energy to be accumulated for processing is constant

- $k_1 \tan(k_2 v + \phi) = d_1$; k_1, k_2 *are constants dependent upon* $E, P_t, P_r, d_0, r_0, \lambda$



- time available for processing is $(d_0 - d_1)/v$

$$t = (f^{-2}\sqrt{(P_r/P_t)}/4\pi c r_0 - tan[k r_0 v * f^2 - tan^{-1}(f^{-2}\sqrt{(P_r/P_t)}/4\pi c)])/v$$



Noise Variance is constant(0.045), velocity=60m/s.

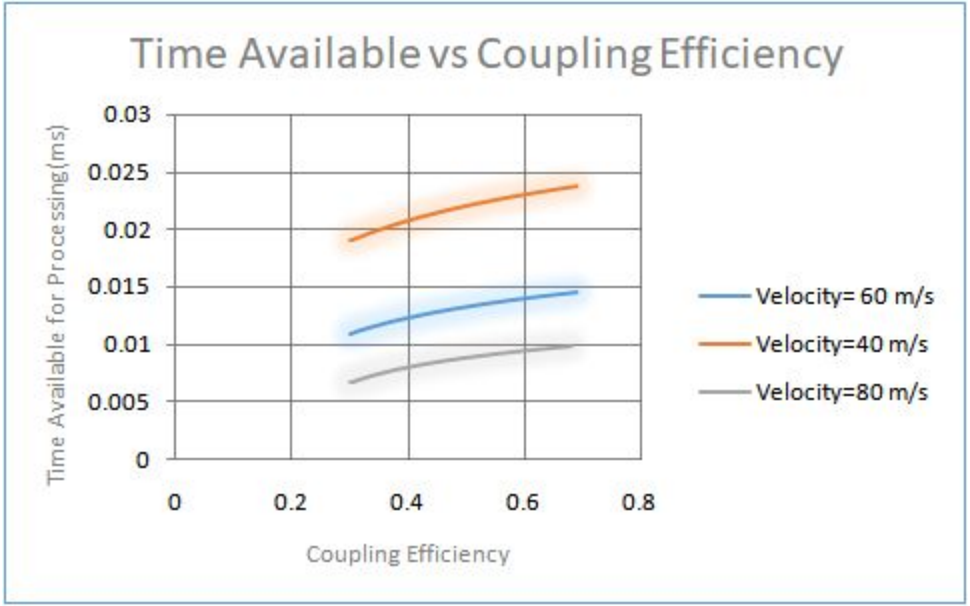


Fig : Pt = 0.5 W ; Noise Variance = 0.045

Implemented Code :

- https://github.com/saurabhkumar8112/SURA_Encryption_Project

References

[1] A. Bogdanov , L.R. Knudsen , G. Leander , C. Paar , A. Poschmann , M.J.B. Robshaw , Y. Seurin , and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", 2007.

[2] J. Harshan, Sang-Yoon Chang, Seungmin Kang, Yih-Chun Hu, ``Securing Balise-based Train Control Systems using Cryptographic Random Fountains,'' in the Proc. of IEEE CNS CPS-sec Workshop 2017, Las Vegas, USA, Oct. 2017.

[3] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen. ``Design and implementation of low-area and low-power AES encryption hardware core", in 9th EUROMICRO Conference on Digital System Design (DSD'06), pages 577–583. IEEE, 2006

[4]M. Katagi and S. Moriai, Lightweight cryptography for the internet of things, Sony Corporation, pages 7–10, 2008

[5] Philip Koopman, Tridib Chakravarty, "Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks", The International Conference on Dependable Systems and Networks, DSN-2004.

[6] Taizo Shirai , Kyoji Shibutani , Toru Akishita , Shiho Moriai , and Tetsu Iwata "The 128-bit Blockcipher CLEFIA", 2007.