Letters

IoT-Based Improved Human Motion Estimations Method Under Cyber Attacks

Md Masud Rana and Rui Bo

***Abstract*—Human beings and control centers are usually far away from each other, so cyber attacks on the sensor measurements can lead to loss of user privacy, information, and trust. Driven by this motivation, this letter proposes an Internet of Things (IoT)-based human motion estimations algorithm under cyber attacks. The sensing measurements are transmitted to the control center over an unreliable communication channel where cyber attack occurs. Based on the mean squared error, the optimal state estimation algorithm is derived to estimate human motions. Simulation results show that the proposed method provides significant performance improvement compared with the existing approach.**

***Index Terms*—Communication channel, control center, cyber attacks, human motion estimations, Internet of Things (IoT), sensors.**

NOMENCLATURE

$\mathbf{A}, \mathbf{A}_d, \mathbf{C}, \mathbf{I}$	Continuous-time state, discrete-time state, observation and identity matrices.
$k, \mathbf{K}, \mathbf{z}$	Time instant, gain and residual error.
$\mathbf{n}, \mathbf{Q}$	Process noise and it covariance matrix.
$\mathbf{v}, \mathbf{R}$	Measurement noise and it covariance matrix.
$\mathbf{x}, \hat{\mathbf{x}}^-, \hat{\mathbf{x}}$	Actual, prior and estimated system states.
$\mathbf{y}, \mu$	Measurements and sampling time.
$\tilde{\mathbf{P}}^-, \tilde{\mathbf{P}}$	Predicted and updated error covariance.

I. INTRODUCTION

CLIENTS and control centers are not co-located, so cyber attacks on the Internet of Things (IoT)-based sensor measurements can cause significant challenges for effectively recognizing human motions such as falling and lying down. The Kalman filter (KF) and extended KF-based human motion estimation method under ideal channel condition is proposed in [1] and [2]. The physiological raw signals from body sensors are processed by the onboard microcontroller, and information is transmitted to the control center [3]. A physician can analyze information and take necessary actions. The idea is then extended in [4], where monitoring center is designed under the IoT network. All the aforementioned algorithms are designed without cyber attacks. Interestingly, there are some relevant attack-resilient algorithms for various cyber-physical system state estimation [5], [6]. Motivated by this, this letter proposes an optimal algorithm for human motion estimations under cyber attacks.

II. HUMAN MOTION SYSTEMS AND MEASUREMENTS

In order to design the monitoring center, a kinematic model of the human leg with measurements by a set of IoT sensors is shown in Fig. 1. This model involves angles and positions of individual limbs and actual forward displacement of the human body [1], [2]. The human motion system and IoT-based sensor measurement are obtained as follows:

$$\mathbf{x}_{k+1} = \mathbf{A}_d \mathbf{x}_k + \mathbf{n}_k \tag{1}$$

$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{v}_k \tag{2}$$

where $\mathbf{x} = [x\ y\ \theta_1\ \omega_1\ \theta_2\ \omega_2]$ is the system state, $\mathbf{A}_d = \mathbf{I} + \mu * \mathbf{A}$, x and y are the horizontal and vertical positions of the foot relative to the hip, θ_1 and ω_1 are the joint angle and angular velocities between the hip and thigh, and θ_2 and ω_2 are the joint angle and angular velocities between the skin and thigh. The continuous-time state $\mathbf{A}$ is a 6 by 6 sparse matrix where the nonzero elements of $\mathbf{A}$ are $A_{14} = -a_1 \sin(\theta_1) - a_2 \sin(\theta_1 + \theta_2)$, $A_{16} = a_2 \sin(\theta_1 + \theta_2)$, $A_{24} = -a_1 \sin(\theta_1) + a_2 \sin(\theta_1 + \theta_2)$, and $A_{26} = a_2 \cos(\theta_1 + \theta_2)$ $A_{34} = A_{56} = 1$. Here, a_1 is the length between the hip and knee, while a_2 is the length between the knee and heel of the foot.

The sensor locally processes raw measurements, and the measurement innovation sequence $\mathbf{z}_k = \mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_k^-$ is transmitted through an additive white Gaussian channel, where cyber attacks are occurred as shown in Fig. 2. The manipulated innovation sequence is $\tilde{\mathbf{z}}_k = \mathbf{T}_k \mathbf{z}_k + \mathbf{a}_k$, where $\mathbf{T}_k$ is the random attacker matrix, and $\mathbf{a}_k$ is the Gaussian channel noise.

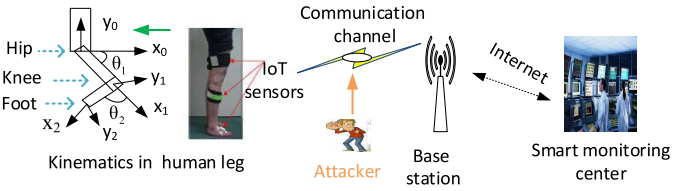

Fig. 1. Proposed IoT-based human motion estimation process.

Fig. 2. Proposed human motion estimations process.

III. PROPOSED ALGORITHM

Theorem 1: Based on the mean squared error principle, the optimal state estimation algorithm is derived. For system state estimation, the optimal gain is derived as follows:

$$\mathbf{K}_k = \tilde{\mathbf{P}}_k \mathbf{C}' \left(\mathbf{C}\tilde{\mathbf{P}}_{\mathbf{C}}' + \mathbf{R} \right)^{-1}. \tag{3}$$

The state prediction and estimation are computed by

$$\tilde{\mathbf{x}}_k^- = \mathbf{A}_d \tilde{\mathbf{x}}_{k-1}, \qquad \tilde{\mathbf{x}}_k = \tilde{\mathbf{x}}_k^- + \mathbf{K}\tilde{\mathbf{z}}_k. \tag{4}$$

Manuscript received June 28, 2019; accepted July 17, 2019. Date of publication August 5, 2019; date of current version December 11, 2019. *(Corresponding author: Md Masud Rana.)*

The authors are with the Department of ECE, Missouri University of Science and Technology, Rolla, MO 65409 USA (e-mail: mrana928@yahoo.com).

Digital Object Identifier 10.1109/JIOT.2019.2932980

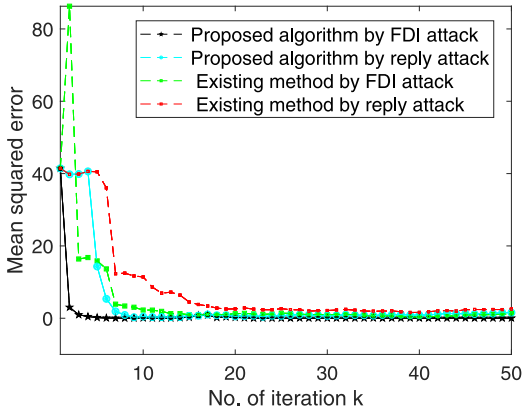

Fig. 3. Performance of the proposed and existing approaches.

The predicted and updated error covariance matrices are [6]

$$\tilde{\mathbf{P}}_k^- = \mathbf{A}_d\tilde{\mathbf{P}}_{k-1}\mathbf{A}_d' + \mathbf{Q}, \quad \tilde{\mathbf{P}}_k = \tilde{\mathbf{P}}_k^- + \bar{\mathbf{P}}\mathbf{C}'\Big(\check{\mathbf{P}} - \mathbf{T}_k'\check{\mathbf{P}} - \check{\mathbf{P}}\mathbf{T}_k\Big)\mathbf{C}\bar{\mathbf{P}}.$$

The gain corrects and minimizes the residual error lead to an accurate estimated system states over time. The proof is derived in Appendix.

IV. Numerical Results and Discussion

The simulation flow chart is shown in Fig. 2. After getting system and measurement by (1) and (2), the optimal gain is computed by (3), which follows the system state estimation and error covariance computation by (4) and (5). For simulation, we consider the false data injection (FDI) and replay attacks. For FDI, the attackers inject malicious information into the targeted network to mislead the control center. In the latter attack, the eavesdropper replays previously recorded measurements thereby trying to move the system into an incorrect state.

The considered process and measurement noises follow Gaussian distributions with mean zero and covariance matrices are being $0.005I$ and $0.02I$, respectively, $a_1 = 0.0882$ m, $a_2 = 0.18$ m, $\theta_i = \pi/180$ Deg, and $\mu = 0.001$ *sec* [1], [2]. During time step $k = 1$ to 10, the eavesdropper attacks the measurement sequences. From simulation result in Fig. 3, it can be seen that the proposed algorithm provides a lower mean squared error between the true and estimated states compared with the existing method in [7]. This is due to the fact that the developed algorithm can effectively reduce estimation errors after computing the optimal gain and error covariance.

V. Conclusion

The optimal estimation algorithm is proposed for human motion estimations. Numerical studies show that the proposed method provides significant performance improvement compared with the existing method.

Appendix
Proof of Theorem 1

The posteriori error covariance is

$$\tilde{\mathbf{P}}_k = E\Big[\big(\mathbf{x}_k - \tilde{\mathbf{x}}_k\big)\big(\mathbf{x}_k - \tilde{\mathbf{x}}_k\big)'\Big] = \tilde{\mathbf{P}}_k^- + \mathbf{K}\big(\mathbf{C}\bar{\mathbf{P}}\mathbf{C}' + \mathbf{R}\big)\mathbf{K}' - E\Big[\Big(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-\Big)\tilde{\mathbf{z}}_k'\mathbf{K}'\Big] - \Big[\mathbf{K}\tilde{\mathbf{z}}_k\Big(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-\Big)'\Big]. \quad (5)$$

Using the mean squared error principle, the above optimal gain is easy to obtain [2], [6]. For the steady-state case, it is assumed that $\tilde{\mathbf{x}}_0^- = \hat{\mathbf{x}}_0^-$ and $\tilde{\mathbf{P}}_0 = E[(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)'] = \bar{\mathbf{P}}$ [6], [7]. Under this assumption, the error term $\mathbf{x}_k - \tilde{\mathbf{x}}_k^-$ in (5) is [6]

$$\mathbf{x}_k - \tilde{\mathbf{x}}_k^- = \mathbf{A}_d^k\Big(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-\Big) + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{n}_{k-1-l} - \sum_{l=0}^{k-1}\mathbf{A}_d^{l+1}\mathbf{K}\tilde{\mathbf{z}}_{k-1-l}^-.$$

Under the same assumption, $\mathbf{x}_k - \hat{\mathbf{x}}_k^-$ can be written as

$$\mathbf{x}_k - \hat{\mathbf{x}}_k^- = \mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})\Big(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^-\Big) + \mathbf{n}_{k-1} - \mathbf{A}_d\mathbf{K}\mathbf{v}_{k-1}.$$

Using above the term $\tilde{\mathbf{z}}_k = \mathbf{T}_k\mathbf{z}_k + \mathbf{a}_k$ can be written as [6]

$$\tilde{\mathbf{z}}_k = \mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^k\big(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-\big) + \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{w}_{k-1-l} + \mathbf{V}.$$

Here, the noisy term $\mathbf{V} = \mathbf{T}_k\mathbf{v}_k + \mathbf{a}_k - \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{A}_d\mathbf{K}\mathbf{v}_{k-1-l}$ and $E(\mathbf{V}) = \mathbf{0}$. $\tilde{\mathbf{z}}_k$ follows an independent identically distributed Gaussian distribution, so orthogonality $E(\tilde{\mathbf{z}}_i\tilde{\mathbf{z}}_j') = \mathbf{0}, \forall i \neq j$, and the third term of (5) can be [6]

$$\begin{aligned}
&E\Big[\Big(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-\Big)\tilde{\mathbf{z}}_k'\mathbf{K}'\Big] \\
&= E\Bigg[\Bigg\{\mathbf{A}_d^k\Big(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-\Big) + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{n}_{k-1-l}\Bigg\} \\
&\qquad \times \Bigg\{\mathbf{T}_k\mathbf{C}\big[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})\big]^k\Big(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-\Big) \\
&\qquad\quad + \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}\big[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})\big]^l\mathbf{w}_{k-1-l}\Bigg\}\mathbf{K}'\Bigg] \\
&= \Bigg\{\mathbf{A}_d^k\bar{\mathbf{P}}\big[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d'\big]^k + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{Q}\big[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d'\big]^l\Bigg\}\mathbf{C}'\mathbf{T}_k'\mathbf{K}' \\
&= \bar{\mathbf{P}}\mathbf{C}'\mathbf{T}_k'\mathbf{K}'. \qquad (6)
\end{aligned}$$

Here, $\bar{\mathbf{P}}$ is the semi-definite matrix [6] which is the composition function of the Lyapunov $h(\mathbf{X})$ and Riccati operator $g(\mathbf{X})$, i.e.,

$$\begin{aligned}
\bar{\mathbf{P}} &= (h \circ g)^k\big(\bar{\mathbf{P}}\big) \\
&= \mathbf{A}_d^k\bar{\mathbf{P}}\big[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d'\big]^k + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{Q}\big[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d'\big]^l. \qquad (7)
\end{aligned}$$

Similarly, the fourth term of (5) can be expressed as [6]

$$E\Big[\mathbf{K}\tilde{\mathbf{z}}_k\Big(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-\Big)'\Big] = \mathbf{K}\mathbf{T}_k\mathbf{C}\bar{\mathbf{P}}. \qquad (8)$$

Substituting (6) and (8) into (5) yields $\tilde{\mathbf{P}}_k$.

References

[1] T. Bennett, R. Jafari, and N. Gans, "An extended Kalman filter to estimate human gait parameters and walking distance," in *Proc. Amer. Control Conf.*, Washington, DC, USA, 2013, pp. 752–757.
[2] A. Olivares, J. Górriz, J. Ramírez, and G. Olivares, "Using frequency analysis to improve the precision of human body posture algorithms based on Kalman filters," *Comput. Biol. Med.*, vol. 72, pp. 229–238, May 2016.
[3] L. Peng, L. Shi, X. Cao, and C. Sun, "Optimal attack energy allocation against remote state estimation," *IEEE Trans. Autom. Control*, vol. 63, no. 7, pp. 2199–2205, Jul. 2018.
[4] Y. Liu and J. Cui, "Design and implementation of human health monitoring platform based on Internet of Things technology," in *Proc. Int. Conf. Comput. Sci. Eng. Embedded Ubiquitous Comput.*, 2017, pp. 422–425.
[5] Q. D. La, T. Q. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016.
[6] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
[7] E. Walach and B. Widrow, "The least mean fourth (LMF) adaptive algorithm and its family," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 2, pp. 275–283, Mar. 1984.